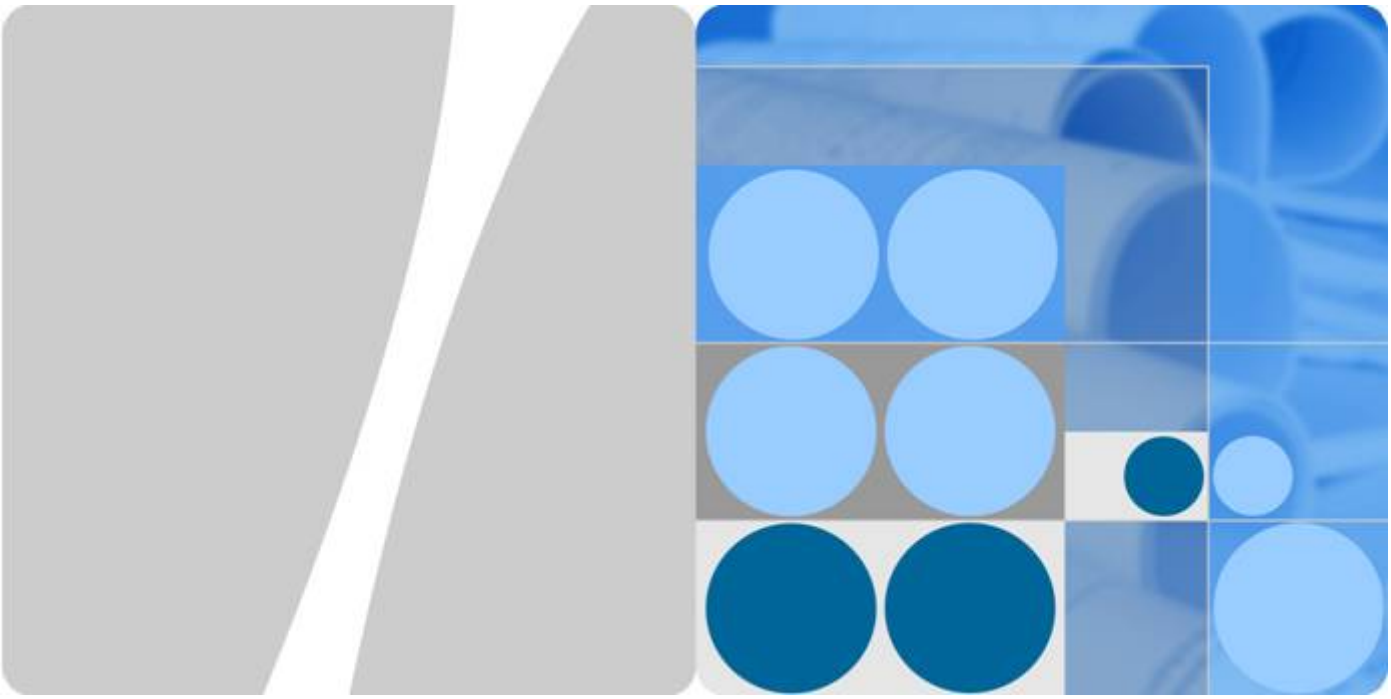


SmartAX MA5600T/MA5603T/MA5608T Multi-service Access Module

V800R015C00

Commissioning and Configuration Guide

Issue 01

Date 2014-04-30

HUAWEI TECHNOLOGIES CO., LTD.

Copyright © Huawei Technologies Co., Ltd. 2014. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Technologies Co., Ltd.

Trademarks and Permissions

and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.
All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between Huawei and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Huawei Technologies Co., Ltd.

Address: Huawei Industrial Base
Bantian, Longgang
Shenzhen 518129
People's Republic of China

Website: http://www.huawei.com

Email: support@huawei.com

Copyright © Huawei Technologies Co., Ltd.

About This Document

Intended Audience

This document describes the commissioning of the basic functions provided by the device in terms of hardware, software, interconnection, and maintenance and management to ensure that the device runs in a stable and reliable state. This document describes the configuration procedures of various services supported by the MA5600T/MA5603T/MA5608T in terms of configuration method and configuration example.

This document helps to learn the commissioning flows, commissioning methods, and configuration procedures of various services of the MA5600T/MA5603T/MA5608T.

This document is intended for:

- Installation and commissioning engineers
- System maintenance engineers
- Data configuration engineers

Symbol Conventions

The following symbols may be found in this document. They are defined as follows

Symbol	Description
DANGER	**DANGER** indicates a hazard with a high level or medium level of risk which, if not avoided, could result in death or serious injury.
WARNING	**WARNING** indicates a hazard with a low level of risk which, if not avoided, could result in minor or moderate injury.
CAUTION	**CAUTION** indicates a potentially hazardous situation that, if not avoided, could result in equipment damage, data loss, performance deterioration, or unanticipated results.
TIP	**TIP** indicates a tip that may help you solve a problem or save time.

Copyright © Huawei Technologies Co., Ltd.

Symbol	Description
NOTE	**NOTE** provides additional information to emphasize or supplement important points of the main text.

Command Conventions

Convention	Description
Boldface	The keywords of a command line are in **boldface**.
Italic	Command arguments are in *italics*.
[ ]	Items (keywords or arguments) in square brackets [ ] are optional.
{ x | y | ... }	Alternative items are grouped in braces and separated by vertical bars. One is selected.
[x | y | ...]	Optional alternative items are grouped in square brackets and separated by vertical bars. One or none is selected.
{ x | y | ... } *	Alternative items are grouped in braces and separated by vertical bars. A minimum of one or a maximum of all can be selected.

GUI Conventions

Convention	Description
Boldface	Buttons, menus, parameters, tabs, window, and dialog titles are in **boldface**. For example, click **OK**.
>	Multi-level menus are in **boldface** and separated by the ">" signs. For example, choose **File** > **Create** > **Folder**

Update History

Updates between document issues are cumulative. Therefore, the latest document issue contains all updates made in previous issues.

Updates in Issue 01 (2014-04-30)

This is the first release. Compared with issue 02 (2013-12-18) of V800R013C10, the document is updated as follows:

Copyright © Huawei Technologies Co., Ltd.

Position	Description
Newly added following chapters in optiCable D-CMTS Configuration (MA5633 Working as a Remote Extended Frame) ● Home Service Networking: – **15.3.1.5 Configuring DHCP Relay (IPv6)** – **15.3.1.6 Configuring a Route (IPv6)** ● L2VPN Enterprise Service Networking: – **15.3.2.5 Configuring DHCP Relay (IPv6)** – **15.3.2.6 Configuring a Route (IPv6)** Newly added following chapters in optiCable D-CMTS Configuration (MA5633 Working as a Standalone NE): **16.3.1.5 Configuring DHCP Relay (IPv6)**	Added the configuration of IPv6.
Modified the following sections in optiCable D-CMTS Configuration (MA5633 Working as a Standalone NE): ● **16.3.1.8 Configuring a Service Channel Between an OLT and a D-CMTS** ● **16.4.1.8 Configuring a Management Channel Between an OLT and a D-CMTS**	Added the configuration of IPv6.

Copyright © Huawei Technologies Co., Ltd.

Contents

About This Document.....ii

1 Commissioning.....1

1.1 Commissioning Introduction.....2
1.1.1 Commissioning Definition.....2
1.1.2 Commissioning Procedure.....2
1.2 Commissioning Preparations.....3
1.2.1 Checking Hardware.....3
1.2.2 Preparing Software.....4
1.2.3 Preparing Tools.....5
1.2.4 Planning Data.....6
1.3 Stand-Alone Commissioning.....7
1.3.1 Checking the Settings of DIP Switches.....7
1.3.1.1 Checking the Settings of DIP Switches on the H801ESC Board.....7
1.3.1.2 Checking the Settings of DIP Switches on the Fan Monitoring Board.....11
1.3.2 Powering On the Device.....16
1.3.3 Commissioning the Power Supply System.....17
1.3.3.1 Checking the Power Supply of the DC PDU.....17
1.3.3.2 Checking the Power Supply of the Power Board.....17
1.3.4 Configuring the Maintenance Terminal.....18
1.3.5 Logging In to the System.....20
1.3.5.1 Login Through the Local Serial Port.....21
1.3.5.2 Login Through Telnet (Outband Management).....26
1.3.5.3 Login Through Telnet (Inband Management).....32
1.3.5.4 Login Through SSH (Outband Management).....38
1.3.5.5 Login Through SSH (Inband Management).....49
1.3.6 Checking the Software State.....61
1.3.7 Loading a Configuration Script.....63
1.3.8 Changing the System Name.....64
1.3.9 Configuring the System Time.....65
1.3.10 Configuring a System User.....67
1.3.10.1 Adding a System User.....67
1.3.10.2 Modifying the System User Attributes.....69

Copyright © Huawei Technologies Co., Ltd.

1.3.11 Configuring a Board....71
1.3.11.1 Adding a Board Offline....72
1.3.11.2 Confirming a Board....73
1.3.11.3 Checking the Board Status....74
1.3.12 Checking the Status of the Upstream Port....75
1.3.13 Checking the Status of the Service Port....75
1.3.14 Enabling the ONT Automatic Discovery function....76
1.3.15 Testing the Optical Power of an Optical Port....76
1.3.15.1 Measuring the Transmit Optical Power of an OLT PON Port....76
1.3.15.2 Measuring the Receive Optical Power of an OLT PON Port....78
1.3.15.3 Measuring the Transmit Optical Power of an ONU PON Port....79
1.3.15.4 Measuring the Receive Optical Power of an ONU PON Port....81
1.3.16 Commissioning the EMU....83
1.3.16.1 Environment Monitoring Application....83
1.3.16.2 Commissioning the EMU_ESC....84
1.3.16.3 Configuring H801VESC Environment Monitoring Parameters....87
1.3.16.4 Configuring the Environment Monitoring Parameters of the EPS30-4815AF....89
1.3.16.5 Configuring the Environment Monitoring Parameters of the EPS75-4815AF....95
1.3.16.6 Configuring the Environment Monitoring Parameters of the GEPS4845....103
1.3.16.7 Configuring the Environment Monitoring Parameters of the ETP4830....109
1.3.16.8 Configuring the Environment Monitoring Parameters of the ETP4890....115
1.3.16.9 Configuring the Power3000 Environment Monitoring Mode....120
1.3.16.10 Commissioning the EMU_TCU....123
1.3.16.11 Commissioning the EMU_FAN....125
1.3.17 Saving and Backing Up Data....127
1.3.17.1 Manually Saving and Backing Up Data....127
1.3.17.2 Configuring the Auto-save and Auto-backup Functions....131
1.4 Interconnection Commissioning....135
1.4.1 Commissioning the Interconnection with the NMS....136
1.4.1.1 Commissioning Outband Network Management (SNMP V1 and V2)....136
1.4.1.2 Commissioning Outband Management (SNMP V3)....143
1.4.1.3 Commissioning Inband Management (SNMP V1 and V2)....149
1.4.1.4 Commissioning Inband Network Management (SNMP V3)....156
1.4.2 Commissioning the Interconnection with the Router....162
1.4.3 Commissioning the Interconnection with the BRAS....163
1.4.4 Interconnection Commissioning of the MG Interface....165
1.4.4.1 Commissioning the Interconnection with the MG Interface(H.248)....165
1.4.4.2 Commissioning the Interconnection with the MG Interface (MGCP)....168
1.4.5 Commissioning the Interconnection with the SIP Interface....171
1.4.6 Commissioning the Management Channel Between the OLT and the GPON MDU....174
1.4.7 Commissioning the Management Channel Between the OLT and the GPON ONT....179

Copyright © Huawei Technologies Co., Ltd.

1.4.8 Commissioning the Management Channel to the xDSL CPE....182
1.5 Maintenance and Management Commissioning....185
1.5.1 Configuring the System Energy-Saving Function....185
1.5.2 Checking Alarms and Events....187
1.5.2.1 Verifying the Alarm and Event Function....187
1.5.2.2 Querying Alarms and Events....187
1.5.3 Checking the Log....190
1.5.4 Checking the System Switchover....191
1.6 Supplementary Information....193
1.6.1 Script Making....193
1.6.2 Configuring the File Transfer Mode....194
1.6.2.1 Configuring the FTP Transfer Mode....195
1.6.2.2 Configuring the SFTP Transfer Mode....196
1.6.2.3 Configuring Xmodem File Transfer Mode....197
1.6.2.4 Configuring the TFTP Transfer Mode....199
1.6.3 Software Package Settings....202
1.6.3.1 Factory Default of the xDSL Line Profile....202
1.6.3.2 Factory Defaults of the xDSL Alarm Profile....207
1.6.3.3 Default settings of the system parameters....209
1.6.3.4 Default settings of the overseas parameters....210
1.6.3.5 Factory Defaults of a DBA Profile....210
1.6.3.6 Default settings of the GPON ONT line profile....213
1.6.3.7 Default settings of the GPON ONT service profile....214
1.6.3.8 Factory Defaults of a GPON ONT Alarm Profile....214
1.6.3.9 Default settings of the environment monitoring units....216

2 Basic Configurations....218

2.1 Configuring Alarms....219
2.2 Adding Port Description....222
2.3 Configuring the Attributes of an Upstream Ethernet Port....223
2.4 Configuring AAA....226
2.4.1 Configuring the Local AAA....227
2.4.2 Configuring the Remote AAA (RADIUS Protocol)....228
2.4.3 Configuration Example of the RADIUS Authentication and Accounting....237
2.4.4 Configuring the Remote AAA (HWTACACS Protocol)....240
2.4.5 Configuration Example of the HWTACACS Authentication (802.1X access user)....244
2.4.6 Configuration Example of HWTACACS Authentication (Management User)....247
2.5 Configuring DOCSIS Event Reporting....250

3 Configuring the DSLAM Services....252

3.1 Example: Configuring the xDSL Internet Access Service....253
3.1.1 Example: Configuring the xDSL Internet Access Service Through PPPoE Dialup....253
3.1.2 Example: Configuring the xDSL IPoE Internet Access Service....260

Copyright © Huawei Technologies Co., Ltd.

3.1.3 Example: Configuring the xDSL PPPoA Internet Access Service....267
3.1.4 Example: Configuring the xDSL IPoA Internet Access Service....273
3.1.5 Example: Configuring the Internet Access Service in the xDSL 802.1X Mode....280
3.1.6 Configuration Example of Changing ADSL Internet Access Service to VDSL Internet Access Service (for the VDSL2 Board)....288
3.2 Example: Configuring the xDSL Multicast Service....292
3.2.1 Configuration Example of the Multicast Video Service (Static Program Configuration)....292
3.2.2 Configuration Example of the Multicast Video Service (Dynamic Program Generation)....297
3.3 Example: Configuring the VoIP Service....301
3.3.1 Example: Configuring the VoIP Service (H.248-based)....301
3.3.2 Example: Configuring the VoIP Service (MGCP-based)....309
3.3.3 Example: Configuring the VoIP PSTN Service (SIP)....316
3.3.4 Example: Configuring the VoIP Service (H.248-based and SIP-based)....323
3.3.5 Example: Configuring the P2P ISDN BRA Service....328
3.3.6 Example: Configuring the P2P ISDN BRA Service (Based on the SIP Protocol)....332
3.3.7 Example: Configuring the P2MP ISDN BRA Service....335
3.3.8 Example: Configuring the P2MP ISDN BRA Service(Based on the SIP Protocol) 338
3.3.9 Example: Configuring the ISDN PRA Service....340
3.3.10 Example: Configuring the ISDN PRA Service (Based on the SIP Protocol)....344
3.3.11 Example: Configuring TDM SHDSL for Carrying the PRA Service....346
3.3.12 Example: Configuring TDM SHDSL for Carrying the PRA Service (Based on the SIP Protocol)....349
3.3.13 Configuring VAGs....351
3.3.13.1 Example: Configuring the H.248/MGCP-based VAG Service....351
3.3.13.2 Example: Configuring the SIP-based VAG Service....358
3.4 Example: Configuring the Triple Play....363
3.4.1 Configuration Example of the Triple Play (Multi-PVC for Multiple Services)....365
3.4.2 Configuration Example of the Triple Play (Single-PVC for Multiple Services) - Stream-based Rate Limitation....372
3.4.3 Configuration Example of the Triple Play Service (Single-PVC for Multiple Services) - User-based and Stream-based Rate Limitation....379

4 Configuration Example of the Private Line Service....388

4.1 Example: Configuring the QinQ VLAN....390
4.2 Example: Configuring VLAN Stacking Multi-ISP Wholesale Access....394
4.3 Configuration Example of the PWE3 Private Line Service....398
4.3.1 Example: Configuring ATM PWE3 to Implement Migration from ATM Network to IP Network....399
4.3.2 Example: Configuring the ATM PWE3 to Achieve emulated ATM Services on the MPLS Network....408
4.3.3 Example: Configuring the ETH PWE3 to Emulate Ethernet Services on the MPLS Network....414
4.3.4 Example: Configuring the TDM PWE3 to Emulate TDM Services on the IP Network....419
4.3.5 Example: Configuring the TDM PWE3 to Emulate TDM Services on the MPLS Network....425
4.4 Configuration Example of TDM SHDSL for Transparently Transmitting the Narrowband Data Private Line Service....430
4.5 Configuration Example of the Private Line Service Leasing E1 Timeslots....433

Copyright © Huawei Technologies Co., Ltd.

5 Configuration Example of MSTP Subtending Network....439
5.1 MSTP Networking....440
5.2 MSTP Dataplan....441
5.3 Configuring MA5600T/MA5603T/MA5608T-1....445
5.4 Configuring MA5600T/MA5603T/MA5608T-2....455
5.5 Configuring MA5600T/MA5603T/MA5608T-3....465
5.6 Configuring MA5600T/MA5603T/MA5608T-4....473
5.7 Configuring MA5600T/MA5603T/MA5608T-5....481
5.8 Verification....487
6 Configuration Example of VPLS....488
6.1 Configuration Example of the VPLS Internet Access Service....490
6.2 Configuration Example of the VPLS Multicast Service....494
6.3 Configuration Example of the VPLS Enterprise Private Line Service....499
7 Example: Subtending Networking....506
7.1 Subtended Network....507
7.2 Data Plan for Subtended Network....508
7.3 Configuring MA5600T-1....511
7.4 Configuring MA5600T-2....520
7.5 Configuring MA5600T-3....530
7.6 Configuring MA5600T-4....537
7.7 Verification....542
8 FTTx Configuration Summary....543
9 FTTH Configuration....546
9.1 FTTH Service Overview....547
9.2 Basic Concepts....547
9.3 Networking Scenarios and Hardware Configurations (GPON)....549
9.4 Networking Scenarios and Hardware Configurations (P2P)....551
9.5 Reference of GPON ONT Capability Sets....552
9.6 Principle of FTTH Data Plan....563
9.6.1 Data Plan Principles for IP Addresses....563
9.6.2 Principle of QoS Planning....564
9.6.3 Principle of Internet Access Service Data Plan....567
9.6.4 Principle of Voice Service Data Plan....569
9.6.5 Principle of IPTV Service Data Plan....573
9.6.6 Principle of Security Data Plan....575
9.7 GPON Access: Configuring FTTH Service....577
9.7.1 Bridging+Voice ONT Network Scenario....578
9.7.1.1 Service Requirements and Application Scenario....578
9.7.1.2 Configuration Process....579
9.7.1.3 Adding an ONT to an OLT....582

Copyright © Huawei Technologies Co., Ltd.

9.7.1.4 Configuring the Internet Access Service....585
9.7.1.5 Configuring the H.248-based Voice Service (on a Web Page or the U2000)....588
9.7.1.6 Configuring the H.248-based Voice Service (Through the CLI)....598
9.7.1.7 Configuring the SIP-based Voice Service (on a Web Page or the U2000)....602
9.7.1.8 Configuring the SIP-based Voice Service (Through the CLI)....611
9.7.1.9 Configuring the BTV Service....616
9.7.1.10 Configuring the VoD Service....619
9.7.1.11 Configuring Link Aggregation, Congestion Control, and Security Policies....621
9.7.1.12 Verifying Services....624
9.7.2 Bridging ONT + HGW Network Scenario....629
9.7.2.1 Service Requirements and Application Scenario....629
9.7.2.2 Configuration Process....630
9.7.2.3 Adding an ONT to an OLT....631
9.7.2.4 Configuring the Internet Access Service....635
9.7.2.5 Configuring the Voice Service....638
9.7.2.6 Configuring the BTV Service....641
9.7.2.7 Configuring the VoD Service....645
9.7.2.8 Configuring Link Aggregation, Congestion Control, and Security Policy....648
9.7.2.9 Verifying Services....651
9.7.3 Gateway ONT Network Scenario....656
9.7.3.1 Service Requirements and Application Scenario....656
9.7.3.2 Configuration Process....657
9.7.3.3 Adding an ONT to an OLT....659
9.7.3.4 Configuring the Internet Access Service (on a Web Page or the U2000)....663
9.7.3.5 Configuring the H.248-based Voice Service (on a Web Page or the U2000)....669
9.7.3.6 Configuring the H.248-based Voice Service (Through the CLI)....679
9.7.3.7 Configuring the SIP-based Voice Service (on a Web Page or the U2000)....683
9.7.3.8 Configuring the SIP-based Voice Service (Through the CLI)....692
9.7.3.9 Configuring the BTV Service....697
9.7.3.10 Configuring the VoD Service....700
9.7.3.11 Configuring Link Aggregation, Congestion Control, and Security Policy....702
9.7.3.12 Verifying Services....705
9.7.4 Configuring Triple Play Service (Simplified Mode)....710
9.8 P2P Access: Configuring FTTH Service....717
10 FTTD Configuration....724
10.1 FTTD Service Overview....725
10.2 Basic Concepts....725
10.3 Networking Scenarios and Hardware Configurations (GPON)....727
10.4 Reference of GPON ONU Capability Sets....730
10.5 Principle of FTTD Data Plan....731
10.5.1 Data Plan Principles for IP Addresses....731

Copyright © Huawei Technologies Co., Ltd.

10.5.2 Principle of QoS Planning....731
10.5.3 Principle of Internet Access Service Data Plan....734
10.5.4 Principle of Voice Service Data Plan....735
10.5.5 Principle of IPTV Service Data Plan....738
10.6 GPON Access: Configuring FTTD Service....740
10.6.1 Bridging+Voice ONU Network Scenario (MA5652S)....740
10.6.1.1 Service Requirements and Application Scenario....741
10.6.1.2 Configuration Process....741
10.6.1.3 Adding an ONU to an OLT....744
10.6.1.4 Configuring a VDSL2 User Port....747
10.6.1.5 Configuring the Internet Access Service....752
10.6.1.6 Configuring the H.248-based Voice Service (Through the CLI)....755
10.6.1.7 Configuring the H.248-based Voice Service (on a Web Page)....759
10.6.1.8 Configuring the SIP-based Voice Service (Through the CLI)....765
10.6.1.9 Configuring the SIP-based Voice Service (on a Web Page)....770
10.6.1.10 Configuring the BTV Service....775
10.6.1.11 Configuring the VoD Service....779
10.6.1.12 Verifying Services....782
10.6.2 Bridging ONU Network Scenario (MA5651/MA5651S)....786
10.6.2.1 Service Requirements and Application Scenario....786
10.6.2.2 Configuration Process....787
10.6.2.3 Adding an ONU to an OLT....788
10.6.2.4 Configuring a VDSL2 User Port....792
10.6.2.5 Configuring the Internet Access Service....797
10.6.2.6 Configuring the Voice Service....800
10.6.2.7 Configuring the BTV Service....803
10.6.2.8 Configuring the VoD Service....807
10.6.2.9 Verifying Services....810
11 FTTB and FTTC Solution Configuration....814
11.1 FTTB and FTTC Service Overview....815
11.1.1 Basic Concept....815
11.1.2 Scenario and Hardware Configuration (GPON)....818
11.1.3 Scenario and Hardware Configuration (10G GPON)....821
11.1.4 Networking Scenarios and Hardware Configurations (Ethernet Cascading)....822
11.1.5 GPON ONU Capability Sets....824
11.1.6 10G GPON ONU Capability Sets....828
11.1.7 Ethernet Upstream ONU Capability Sets....829
11.2 Principle of FTTB and FTTC Data Plan....833
11.2.1 Principle of Device Management Data Plan....833
11.2.2 Principle of QoS Data Plan....835
11.2.3 Principle of Internet Access Service Data Plan....837

Copyright © Huawei Technologies Co., Ltd.

11.2.4 (Optional) Principle of Vectoring Data Plan....840
11.2.5 Principle of VoIP Service Data Plan....842
11.2.6 Principle of IPTV Service Data Plan....846
11.2.7 Principle of Security Data Plan....854
11.3 Configuring Services in Various FTTB and FTTC Scenarios (GPON and 10G GPON Access)....856
11.3.1 FTTB Networking (LAN Access Without HGW)....857
11.3.1.1 Service Requirements and Application Scenarios....857
11.3.1.2 Configuration Procedure....858
11.3.1.3 Adding an ONU to an OLT....860
11.3.1.4 Configuring the Management Channel Between the OLT and the ONU....864
11.3.1.5 Configuring the Service Channel Between the OLT and the ONU....865
11.3.1.6 Configuring LAN Internet Access Service (On the ONU)....867
11.3.1.7 Configuring H.248 Voice Service (on the ONU)....869
11.3.1.8 Configuring SIP Voice Service (on the ONU)....872
11.3.1.9 Configuring Link Aggregation, Congestion Control, and Security Policies....876
11.3.1.10 Verifying Services....879
11.3.2 FTTB/C Networking (xDSL Access, Without HGW)....881
11.3.2.1 Service Requirements and Application Scenario....881
11.3.2.2 Configuration Procedure....882
11.3.2.3 Adding an ONU to an OLT....884
11.3.2.4 Configuring the Management Channel Between the OLT and the ONU....888
11.3.2.5 Configuring the Service Channel Between the OLT and the ONU....889
11.3.2.6 Configuring the Internet Access Service (ADSL2+ Access, on the ONU)....891
11.3.2.7 Configuring the Internet Access Service (VDSL2 Access, on the ONU)....894
11.3.2.8 (Optional) Configuring Vectoring....897
11.3.2.9 Configuring H.248 Voice Service (on the ONU)....908
11.3.2.10 Configuring SIP Voice Service (on the ONU)....912
11.3.2.11 Configuring Link Aggregation, Congestion Control, and Security Policy....915
11.3.2.12 Verifying Services....918
11.3.3 FTTB/FTTC+HGW Networking (Voice Service Provided by ONU)....920
11.3.3.1 Service Requirements and Application Scenario....920
11.3.3.2 Configuration Procedure....922
11.3.3.3 Adding an ONU to an OLT....925
11.3.3.4 Configuring the Management Channel Between the OLT and the ONU....929
11.3.3.5 Configuring Service Channels Between an OLT and an ONU....930
11.3.3.6 Configuring the Internet Access Service (LAN Access, on the ONU)....934
11.3.3.7 Configuring the Internet Access Service (ADSL2+ Access, on the ONU)....935
11.3.3.8 Configuring the Internet Access Service (VDSL2 Access, on the ONU)....938
11.3.3.9 (Optional) Configuring Vectoring....941
11.3.3.10 Configuring H.248 Voice Service (on the ONU)....952
11.3.3.11 Configuring SIP Voice Service (on the ONU)....956

Copyright © Huawei Technologies Co., Ltd.

11.3.3.12 Configuring the IPTV Service (on the ONU).....959
11.3.3.13 Configuring Link Aggregation, Congestion Control, and Security Policy.....962
11.3.3.14 Configuring the Internet Access Service (on the HGW).....965
11.3.3.15 Configuring the IPTV Service (on the HGW).....967
11.3.3.16 Verifying Services.....969
11.3.4 FTTB/FTTC+HGW Networking (HGW Providing the VoIP Service).....973
11.3.4.1 Service Requirements and Application Scenario.....973
11.3.4.2 Configuration Procedure.....974
11.3.4.3 Adding an ONU to an OLT.....977
11.3.4.4 Configuring the Management Channel Between the OLT and the ONU.....981
11.3.4.5 Configuring the Service Channel Between the OLT and the ONU.....982
11.3.4.6 Configuring the Internet Access Service (LAN Access, on the ONU).....986
11.3.4.7 Configuring the Internet Access Service (ADSL2+ Access, on the ONU).....987
11.3.4.8 Configuring the Internet Access Service (VDSL2 Access, on the ONU).....990
11.3.4.9 (Optional) Configuring Vectoring.....993
11.3.4.10 Configuring the Voice Service Channel (on the ONU).....1004
11.3.4.11 Configuring the IPTV Service (on the ONU).....1006
11.3.4.12 Configuring Link Aggregation, Congestion Control, and Security Policy.....1009
11.3.4.13 Configuring the Internet Access Service (on the HGW).....1012
11.3.4.14 Configuring the IPTV Service (on the HGW).....1014
11.3.4.15 Configuring the VoIP Service (on the HGW).....1016
11.3.4.16 Verifying Services.....1019
11.4 Configuring Services in Various FTTB and FTTC Scenarios (Ethernet Cascading).....1022
11.4.1 FTTB and FTTC Ethernet Cascade Networking (ONU Works as an Independent NE).....1022
11.4.1.1 Service Requirements and Usage Scenario.....1022
11.4.1.2 Configuration Procedure.....1024
11.4.1.3 Configuring the Working Mode of an Ethernet Cascading Board.....1025
11.4.1.4 Configuring the Management Channel Between an OLT and an ONU.....1026
11.4.1.5 Configuring the Service Channel Between an OLT and an ONU.....1032
11.4.1.6 Configuring the Service Flow on an ONU or HGW.....1036
11.4.1.7 Configuring Link Aggregation, Congestion Control, and Security Policy.....1039
11.4.1.8 Verifying Services.....1042
11.4.2 FTTB and FTTC Ethernet Cascade Networking (ONU works as a GE remote extended subrack).....1043
11.4.2.1 Service Requirements and Application Scenarios for GE Remote Extended Subrack.....1043
11.4.2.2 Principle of Data Planning for GE Remote Extended Subrack.....1044
11.4.2.3 Configuration Procedure for GE Remote Extended Subrack.....1046
11.4.2.4 Adding GE Remote Extended Subracks.....1048
11.4.2.5 Configuring VDSL2 User Ports.....1049
11.4.2.6 Configuring VDSL2 Service Flows.....1050
11.4.2.7 (Optional) Configuring Vectoring.....1053
11.4.2.8 Configuring Link Aggregation, Congestion Control, and Security Policies.....1059

Copyright © Huawei Technologies Co., Ltd.

11.4.2.9 Configuring the Internet Access Service (on the HGW).....1063
11.4.2.10 Configuring the IPTV Service (on the HGW).....1065
11.4.2.11 Configuring the VoIP Service (on the HGW).....1067
11.4.2.12 Verifying Services.....1069
12 FTTO Configuration(SOHO and SME).....1073
12.1 Overview of FTTO Services (SOHO and SME).....1074
12.1.1 Basic Concept.....1074
12.1.2 Networking Scenario and Hardware Configurations.....1076
12.1.3 ONU Capability Sets.....1078
12.2 Principles of Planning Data for FTTO Services (SOHO and SME).....1080
12.2.1 Principles of Planing Device Management Data.....1080
12.2.2 Principle of QoS Planning.....1082
12.2.3 Principle of Internet Access Service Data Plan.....1085
12.2.4 Principles of Planning Voice Service Data.....1086
12.2.5 Principle of IPTV Service Data Plan.....1090
12.2.6 Principle of Security Data Plan.....1091
12.2.7 Principle of Reliability Data Plan.....1094
12.3 SOHO Service Configuration (GPON).....1096
12.3.1 Service Requirements and Usage Scenario.....1096
12.3.2 Configuration Procedure.....1098
12.3.3 Adding an ONU to an OLT.....1099
12.3.4 Configuring the Internet Access Service.....1103
12.3.5 Configuring the H.248-based Voice Service (on a Web Page).....1107
12.3.6 Configuring the H.248-based Voice Service (Through the CLI).....1114
12.3.7 Configuring the SIP-based Voice Service (on a Web Page).....1119
12.3.8 Configuring the SIP-based Voice Service (Through the CLI).....1126
12.3.9 Configuring the BTV Service.....1131
12.3.10 Configuring the VoD Service.....1134
12.3.11 Configuring Link Aggregation, Congestion Control, and Security Policy.....1135
12.3.12 Verifying Services.....1138
12.4 SME Service Configuration (GPON).....1143
12.4.1 Bridging and Router Networking.....1143
12.4.1.1 Service Requirements and Usage Scenario.....1143
12.4.1.2 Configuration Procedure.....1144
12.4.1.3 Adding an ONU to an OLT 1146
12.4.1.4 Configuring the Internet Access Service.....1150
12.4.1.5 Configuring the H.248-based Voice Service (on a Web Page).....1152
12.4.1.6 Configuring the H.248-based Voice Service (Through the CLI).....1159
12.4.1.7 Configuring the SIP-based Voice Service (on a Web Page).....1162
12.4.1.8 Configuring the SIP-based Voice Service (Through the CLI).....1169
12.4.1.9 Configuring the BTV Service.....1174

Copyright © Huawei Technologies Co., Ltd.

12.4.1.10 Configuring the VoD Service....1177
12.4.1.11 Configuring Link Aggregation, Congestion Control, and Security Policy....1180
12.4.1.12 Verifying Services....1183
12.4.2 Gateway Networking....1187
12.4.2.1 Service Requirements and Usage Scenario....1187
12.4.2.2 Configuration Procedure....1188
12.4.2.3 Adding an ONU to an OLT....1190
12.4.2.4 Configuring the Internet Access Service....1194
12.4.2.5 Configuring the H.248-based Voice Service (on a Web Page)....1198
12.4.2.6 Configuring the H.248-based Voice Service (Through the CLI)....1205
12.4.2.7 Configuring the SIP-based Voice Service (on a Web Page)....1209
12.4.2.8 Configuring the SIP-based Voice Service (Through the CLI)....1216
12.4.2.9 Configuring the BTV Service....1222
12.4.2.10 Configuring the VoD Service....1225
12.4.2.11 Configuring Link Aggregation, Congestion Control, and Security Policy....1226
12.4.2.12 Verifying Services....1229
12.4.3 Layer 2 Interoperation Service Between Enterprise Branches....1234
12.4.3.1 Service Requirement and Application Scenario....1234
12.4.3.2 Configuration Procedure....1235
12.4.3.3 Adding ONUs to OLT....1237
12.4.3.4 Configuring Layer 2 Interoperation Service Ports on OLT....1241
12.4.3.5 Configuring Congestion Control and Security Policies....1242
12.4.3.6 Configuring E2E Reliability....1243
12.4.3.7 Verifying Services....1247

13 FTTO Configuration (Large-sized Enterprise Access)....1250

13.1 Overview of Enterprise Access Service....1251
13.1.1 Basic Concepts....1251
13.1.2 Networking Scenarios and Hardware Configurations (GPON)....1254
13.1.3 GPON ONU Capability Set....1255
13.2 Principle of Planning Data for Enterprise Access Service....1257
13.2.1 Principle of Equipment Management Data Plan....1257
13.2.2 Principle of VLAN Data Plan....1258
13.2.3 Principle of QoS Data Plan....1260
13.2.4 Principle of Protocol Transparent Transmission Data Plan....1263
13.2.5 Principle of Security Data Plan....1264
13.2.6 Principle of Reliability Data Plan....1266
13.3 Configuring Enterprise Access Service (GPON)....1268
13.3.1 Layer 2 Interoperation Service Between Enterprise Branches....1269
13.3.1.1 Service Requirement and Application Scenario....1269
13.3.1.2 Configuration Process....1270
13.3.1.3 Adding ONUs to OLT....1271

Copyright © Huawei Technologies Co., Ltd.

13.3.1.4 Configuring Management Service Ports on OLT and ONUs....1275
13.3.1.5 Configuring Layer 2 Interoperation Service Ports on OLT....1276
13.3.1.6 Configuring Ethernet Access Service Ports on ONUs....1278
13.3.1.7 Configuring Congestion Control and Security Policies....1279
13.3.1.8 Configuring E2E Reliability....1281
13.3.1.9 Verifying Services....1285
13.3.2 Enterprise DDN Private Line Access Service....1287
13.3.2.1 Service Requirement and Application Scenario....1287
13.3.2.2 Configuration Process....1288
13.3.2.3 Adding ONUs to OLT....1289
13.3.2.4 Configuring Management Service Ports on OLT and ONUs....1292
13.3.2.5 Configuring TDM Connections....1293
13.3.2.6 Configuring Clock Synchronization....1294
13.3.2.7 Verifying Services....1296
13.3.3 Enterprise IP PBX Private Line Access Service....1299
13.3.3.1 Service Requirement and Application Scenario....1299
13.3.3.2 Configuration Process....1300
13.3.3.3 Adding ONUs to OLT....1301
13.3.3.4 Configuring Management Service Ports on OLT and ONUs....1303
13.3.3.5 Configuring OLT QinQ Service Ports....1304
13.3.3.6 Configuring Ethernet Access Service Ports on ONUs....1305
13.3.3.7 Configuring Congestion Control and Security Policies....1306
13.3.3.8 Configuring E2E Reliability....1308
13.3.3.9 Verifying Services....1312
13.3.4 Enterprise PRA PBX Private Line Access Service....1313
13.3.4.1 Service Requirement and Application Scenario....1313
13.3.4.2 Configuration Process....1314
13.3.4.3 Adding ONUs to OLT....1314
13.3.4.4 Configuring Management Service Ports on OLT and ONUs....1317
13.3.4.5 Configuring Service Ports for Voice Transparent Transmission....1318
13.3.4.6 Configuring VoIP PRA Access....1319
13.3.4.7 Configuring Congestion Control and Security Policies....1322
13.3.4.8 Configuring E2E Reliability....1323
13.3.4.9 Verifying Services....1327
13.3.5 Enterprise E1 Unified Access Service....1328
13.3.5.1 Service Requirement and Application Scenario....1328
13.3.5.2 Configuration Process....1328
13.3.5.3 Adding ONUs to OLT....1330
13.3.5.4 Configuring Management Service Ports on OLT and ONUs....1332
13.3.5.5 Configuring SAToP Connections and Service Ports....1333
13.3.5.6 Configuring ONU SAToP Connections....1336

Copyright © Huawei Technologies Co., Ltd.

13.3.5.7 Configuring Clock Synchronization....1337
13.3.5.8 Configuring Congestion Control and Security Policies....1339
13.3.5.9 Configuring Network Protectio....1341
13.3.5.10 Verifying Services....1343
13.3.6 Enterprise E1/T1 Unified Access Service (OLT Cascading)....1345
13.3.6.1 Service Requirement and Application Scenario....1345
13.3.6.2 Configuration Process....1346
13.3.6.3 Configure OLT_A cascading with OLT_B....1347
13.3.6.4 Configuring SAToP Connections between OLT_A and ONU....1348
13.3.6.5 Adding ONUs to OLT_B....1349
13.3.6.6 Configuring Management and Service Channel on OLT_B and ONU....1352
13.3.6.7 Configuring ONU SAToP Connections....1353
13.3.6.8 Configuring Clock Synchronization....1355
13.3.6.9 Verifying Services....1357
14 FTTM Configuration (Base Station Access)....1360
14.1 Overview of Base Station Access Service....1361
14.1.1 Basic Concepts....1361
14.1.2 Networking Scenarios and Hardware Configurations (GPON)....1362
14.1.3 GPON ONU Capability Set....1364
14.2 Prinpicle of Planning Data for Base Station Access Service....1366
14.2.1 Principle of Equipment Management Data Plan....1366
14.2.2 Principle of VLAN Data Plan....1367
14.2.3 Principle of QoS Data Plan....1369
14.2.4 Principle of Clock Synchronization Data Plan....1370
14.2.5 Principle of Security Data Plan....1372
14.2.6 Planning Reliability Data....1373
14.3 Configuring Base station access Clock Synchronization....1376
14.3.1 Overview of Base station access Clock/Time Synchronization....1376
14.3.2 Configuring BITS Clock Synchronization....1381
14.3.3 Configuring E1/STM-1 Line Clock Synchronization....1384
14.3.4 Configuring Ethernet Clock Synchronization....1386
14.3.5 Configuring "1PPS+ToD" Clock Synchronization....1389
14.3.6 Configuring 1588v2 Clock Synchronization....1393
14.4 Configuring Base Station Access Service (GPON)....1399
14.4.1 E1 Base Station Access Service (in Native TDM Mode)....1399
14.4.1.1 Service Requirement and Application Scenario....1399
14.4.1.2 Configuration Process....1400
14.4.1.3 Adding ONUs to OLT....1401
14.4.1.4 Configuring Management Service Ports on OLT and ONUs....1404
14.4.1.5 Configuring TDM E1 Connections....1405
14.4.1.6 Configuring Clock Synchronization....1406

Copyright © Huawei Technologies Co., Ltd.

14.4.1.7 Configuring Congestion Control and Security Policies....1408
14.4.1.8 Configuring Network Protection....1410
14.4.1.9 Verifying Services....1411
14.4.2 E1 Base Station Access Service (in SAToP Mode)....1414
14.4.2.1 Service Requirement and Application Scenario....1414
14.4.2.2 Configuration Process....1415
14.4.2.3 Adding ONUs to OLT....1417
14.4.2.4 Configuring Management Service Ports on OLT and ONUs....1419
14.4.2.5 Configuring SAToP Connections and Service Ports....1420
14.4.2.6 Configuring Clock Synchronization....1423
14.4.2.7 Configuring Congestion Control and Security Policies....1425
14.4.2.8 Configuring Network Protection....1426
14.4.2.9 Configuring ONU SAToP Connections....1428
14.4.2.10 Verifying Services....1430
14.4.3 Ethernet Base Station Access Service (in QinQ VLAN Mode)....1432
14.4.3.1 Service Requirement and Application Scenario....1432
14.4.3.2 Configuration Process....1433
14.4.3.3 Adding ONUs to OLT....1434
14.4.3.4 Configuring Management Service Ports on OLT and ONUs....1437
14.4.3.5 Configuring OLT QinQ VLANs and Service Ports....1438
14.4.3.6 Configuring Ethernet Access Service Ports on ONUs....1440
14.4.3.7 Configuring Clock Synchronization....1442
14.4.3.8 Configuring Congestion Control and Security Policies....1443
14.4.3.9 Configuring Network Protection....1445
14.4.3.10 Verifying Services....1449
14.4.4 Symmetrical TDM PWE3 Access for OLTs on Both Sides....1449
14.4.4.1 Service Requirements and Application Scenario....1449
14.4.4.2 Configuration Procedure....1450
14.4.4.3 Adding ONUs to the OLT and Configuring the Management Service Port....1451
14.4.4.4 Configuring the TDM Connection and TDM PW....1454
14.4.4.5 Configuring Clock Synchronization....1457
14.4.4.6 Configuring Congestion Control and Security Policies....1458
14.4.4.7 Configuring E2E Reliability....1460
14.4.4.8 Verifying Services....1464
14.4.5 GPON Access for the OLT one Side and E1 or SHDSL access for the OLT on the Peer Side....1465
14.4.5.1 Service Requirements and Application Scenario....1465
14.4.5.2 Configuration Procedure....1466
14.4.5.3 Adding ONUs to OLT-A and Configuring the Management Service Port....1466
14.4.5.4 Configuring the TDM Connection and TDM PW....1470
14.4.5.5 Configuring Clock Synchronization....1473
14.4.5.6 Configuring E2E Reliability....1474

Copyright © Huawei Technologies Co., Ltd.

14.4.5.7 Verifying Services....1478
14.4.6 Symmetrical E1 or SHDSL Access for OLTs on Both Sides....1479
14.4.6.1 Service Requirements and Application Scenario....1479
14.4.6.2 Configuration Procedure....1480
14.4.6.3 Configuring the TDM Connection and TDM PW....1480
14.4.6.4 Configuring Clock Synchronization....1483
14.4.6.5 Verifying Services....1484
14.4.7 E1 Access for the ONU and TDM PWE3 Between the ONU and Peer PE....1486
14.4.7.1 Service Requirements and Application Scenario....1486
14.4.7.2 Configuration Procedure....1486
14.4.7.3 Adding ONUs to the OLT and Configuring the Management Service Port....1487
14.4.7.4 Configuring the TDM VCL and CESoP Connection on the ONU....1490
14.4.7.5 Configuring the Static LSP and PW on the CX600....1492
14.4.7.6 Configuring Clock Synchronization....1493
14.4.7.7 Verifying Services....1495
14.4.8 Small-Cell Base Station Access Service (in QinQ VLAN through CLI Configuration)....1496
14.4.8.1 Service Requirements and Application Scenarios....1496
14.4.8.2 Configuration Procedure....1497
14.4.8.3 Configuring Ethernet Access Service Ports on ONUs....1497
14.4.8.4 Configuring Congestion Control and Security Policies....1499
14.4.8.5 Configuring Clock Synchronization....1500
14.4.8.6 Configuring End to End Protection....1502
14.4.8.7 Verifying Services....1503
14.4.9 Small-Cell Base Station Access Service (in QinQ VLAN Mode Through GUI Pre-Deployment)....1503
14.4.9.1 Service Requirements and Application Scenarios....1504
14.4.9.2 Configuration Procedure....1504
14.4.9.3 Configuring the IP Address of the NMS Server and the IP Address Pool of the ONU (GPON Dock Scenario)....1505
14.4.9.4 Creating the Authentication-Free Policy and Associating It with the OLT (GPON Dock Scenario)....1507
14.4.9.5 Configuring the Remote Software Commissioning Policy (GPON Dock Scenario)....1511
14.4.9.6 Configuring Clock Synchronization....1512
14.4.9.7 Verifying Services....1514
15 OptiCable D-CMTS Configuration (MA5633 Working as a Remote Extended Frame)....1515
15.1 D-CMTS Service Overview....1517
15.1.1 Basic Concepts....1517
15.1.2 Networking Scenarios and Hardware Configurations (GPON)....1522
15.1.3 Networking Scenarios and Hardware Configurations (GE)....1523
15.2 Data Plan Principles for D-CMTS Services....1524
15.2.1 Frequency Spectrum Management....1524
15.2.2 Device Management....1526

Copyright © Huawei Technologies Co., Ltd.

15.2.3 QoS....1526
15.2.4 VLAN....1530
15.2.5 VLAN Planning for Telecom Networks....1532
15.3 Service Configuration on a D-CMTS That Works as a GPON Remote Extended Frame on a Layer 3 Network....1535
15.3.1 Home Service Networking....1536
15.3.1.1 Service Requirements and Usage Scenario....1536
15.3.1.2 Configuration Process....1537
15.3.1.3 Configuring DHCP Relay....1540
15.3.1.4 Configuring a Route....1542
15.3.1.5 Configuring DHCP Relay (IPv6)....1544
15.3.1.6 Configuring a Route (IPv6)....1547
15.3.1.7 Adding a Remote Extended Frame to an OLT....1549
15.3.1.8 Configuring RF Port Parameters....1552
15.3.1.9 Configuring the HSI Service....1556
15.3.1.10 Configuring the DOCSIS VoD Service....1557
15.3.1.11 Configuring the EQAM VoD Service....1558
15.3.1.12 Configuring the BTV Service....1561
15.3.1.13 Configuring the Dynamic PacketCable Service....1563
15.3.1.14 Verifying Services....1564
15.3.2 L2VPN Enterprise Service Networking....1569
15.3.2.1 Service Requirements and Usage Scenario....1569
15.3.2.2 Configuration Process....1570
15.3.2.3 Configuring DHCP Relay....1571
15.3.2.4 Configuring a Route....1573
15.3.2.5 Configuring DHCP Relay (IPv6)....1575
15.3.2.6 Configuring a Route (IPv6)....1577
15.3.2.7 Adding a Remote Extended Frame to an OLT....1579
15.3.2.8 Configuring RF Port Parameters....1581
15.3.2.9 Configuring the L2VPN Enterprise Service....1585
15.3.2.10 Verifying Services....1586
15.3.3 WLAN Hotspot Radio Backhaul Service Networking....1590
15.4 Service Configuration on a D-CMTS That Works as a GE Remote Extended Frame on a Layer 3 Network....1591
15.4.1 Home Service Networking....1592
15.4.1.1 Service Requirements and Usage Scenario....1592
15.4.1.2 Configuration Process....1593
15.4.1.3 Configuring DHCP Relay....1595
15.4.1.4 Configuring a Route....1598
15.4.1.5 Configuring DHCP Relay (IPv6)....1600
15.4.1.6 Configuring a Route (IPv6)....1603
15.4.1.7 Adding a Remote Extended Frame to an OLT....1605
15.4.1.8 Configuring RF Port Parameters....1607

Copyright © Huawei Technologies Co., Ltd.

15.4.1.9 Configuring the HSI Service....1611
15.4.1.10 Configuring the DOCSIS VoD Service....1612
15.4.1.11 Configuring the EQAM VoD Service....1613
15.4.1.12 Configuring the BTV Service....1616
15.4.1.13 Configuring the Dynamic PacketCable Service....1618
15.4.1.14 Verifying Services....1619
15.4.2 L2VPN Enterprise Service Networking....1624
15.4.2.1 Service Requirements and Usage Scenario....1624
15.4.2.2 Configuration Process....1624
15.4.2.3 Configuring DHCP Relay....1626
15.4.2.4 Configuring a Route....1628
15.4.2.5 Configuring DHCP Relay (IPv6)....1629
15.4.2.6 Configuring a Route (IPv6)....1631
15.4.2.7 Adding a Remote Extended Frame to an OLT....1633
15.4.2.8 Configuring RF Port Parameters....1636
15.4.2.9 Configuring the L2VPN Enterprise Service....1639
15.4.2.10 Verifying Services....1641
15.4.3 WLAN Hotspot Radio Backhaul Service Networking....1644
15.5 Service Configuration on a D-CMTS That Works as a GPON Remote Extended Frame on a Layer 2 Telecom Network....1645
15.5.1 Home Service Networking....1646
15.5.1.1 Service Requirements and Usage Scenario....1646
15.5.1.2 Configuration Process....1647
15.5.1.3 Adding a Remote Extended Frame to an OLT....1649
15.5.1.4 Configuring RF Port Parameters....1652
15.5.1.5 Configuring the HSI Service....1655
15.5.1.6 Configuring the DOCSIS VoD Service....1656
15.5.1.7 Verifying Services....1657
16 OptiCable D-CMTS Configuration (MA5633 Working as a Standalone NE)....1662
16.1 D-CMTS Service Overview....1664
16.1.1 Basic Concepts....1664
16.1.2 Networking Scenarios and Hardware Configurations....1668
16.2 Data Plan Principles for D-CMTS Services....1669
16.2.1 Frequency Spectrum Management....1669
16.2.2 Device Management....1671
16.2.3 QoS....1672
16.2.4 VLAN....1675
16.3 Service Configuration on a D-CMTS That Works in GE Access Mode on a Layer 3 Network....1679
16.3.1 Home Service Networking....1679
16.3.1.1 Service Requirements and Usage Scenario....1679
16.3.1.2 Configuration Process....1680

Copyright © Huawei Technologies Co., Ltd.

16.3.1.3 Configuring DHCP Relay....1683
16.3.1.4 Configuring a Route....1685
16.3.1.5 Configuring DHCP Relay (IPv6)....1687
16.3.1.6 Configuring a Route (IPv6)....1689
16.3.1.7 Configuring a Management Channel Between an OLT and a D-CMTS....1692
16.3.1.8 Configuring a Service Channel Between an OLT and a D-CMTS....1694
16.3.1.9 Configuring RF Port Parameters on a D-CMTS....1696
16.3.1.10 Configuring the HSI Service on a D-CMTS....1698
16.3.1.11 Configuring the DOCSIS VoD Service on a D-CMTS....1699
16.3.1.12 Configuring the EQAM VoD Service on a D-CMTS....1700
16.3.1.13 Configuring the BTV Service....1703
16.3.1.14 Configuring the Dynamic PacketCable Service on a D-CMTS....1705
16.3.1.15 Verifying Services....1707
16.3.2 L2VPN Enterprise Service Networking....1711
16.3.2.1 Service Requirements and Usage Scenario....1711
16.3.2.2 Configuration Process....1711
16.3.2.3 Configuring DHCP Relay....1713
16.3.2.4 Configuring a Route....1714
16.3.2.5 Configuring DHCP Relay (IPv6)....1716
16.3.2.6 Configuring a Route (IPv6)....1718
16.3.2.7 Configuring a Management Channel Between an OLT and an MA5633....1720
16.3.2.8 Configuring a Service Channel Between an OLT and a D-CMTS....1722
16.3.2.9 Configuring RF Port Parameters on an MA5633....1724
16.3.2.10 Configuring the L2VPN Enterprise Service(on the CMC)....1726
16.3.2.11 Verifying Services....1727
16.3.3 WLAN Hotspot Radio Backhaul Service Networking....1731
16.4 Service Configuration on a D-CMTS That Works in GPON Access Mode on a Layer 3 Network....1732
16.4.1 Home Service Networking....1733
16.4.1.1 Service Requirements and Usage Scenario....1733
16.4.1.2 Configuration Process....1734
16.4.1.3 Configuring DHCP Relay....1736
16.4.1.4 Configuring a Route....1739
16.4.1.5 Configuring DHCP Relay (IPv6)....1741
16.4.1.6 Configuring a Route (IPv6)....1743
16.4.1.7 Adding a D-CMTS to an OLT....1745
16.4.1.8 Configuring a Management Channel Between an OLT and a D-CMTS....1750
16.4.1.9 Configuring a Service Channel Between an OLT and a D-CMTS....1751
16.4.1.10 Configuring RF Port Parameters on an MA5633....1753
16.4.1.11 Configuring the HSI Service on an MA5633....1755
16.4.1.12 Configuring the DOCSIS VoD Service on an MA5633....1756
16.4.1.13 Configuring the EQAM VoD Service on an MA5633....1757

Copyright © Huawei Technologies Co., Ltd.

16.4.1.14 Configuring the BTV Service on an MA5633....1760
16.4.1.15 Configuring the Dynamic PacketCable Service on an MA5633....1762
16.4.1.16 Verifying Services....1764
16.4.2 L2VPN Enterprise Service Networking....1768
16.4.2.1 Service Requirements and Usage Scenario....1768
16.4.2.2 Configuration Process....1768
16.4.2.3 Configuring DHCP Relay....1771
16.4.2.4 Configuring a Route....1772
16.4.2.5 Configuring DHCP Relay (IPv6)....1774
16.4.2.6 Configuring a Route (IPv6)....1776
16.4.2.7 Adding a D-CMTS to an OLT....1778
16.4.2.8 Configuring a Management Channel Between an OLT and an MA5633....1782
16.4.2.9 Configuring a Service Channel Between an OLT and a D-CMTS....1784
16.4.2.10 Configuring RF Port Parameters on an MA5633....1786
16.4.2.11 Configuring the L2VPN Enterprise Service on an MA5633....1788
16.4.2.12 Verifying Services....1789
16.4.3 WLAN Hotspot Radio Backhaul Service Networking....1793

17 Electrical Service Configuration....1795

17.1 Configuration Example of the FTTx Service (GPON Access)....1796
17.1.1 Configuration Example of Transmitting Video Monitoring Data over Ethernet Access....1796
17.1.2 Configuration Example of Intelligently Collecting Power Consumption Information over Ethernet Access....1805
17.1.3 Configuration Example of Automatically Transmitting Site Information over Ethernet (Single Homing)....1814
17.1.4 Configuration Example of Automatically Transmitting Site Information over Ethernet (Dual Homing)....1831
17.1.5 Configuration Example of Transmitting Information Collected in Centralized Mode in the Smart Grid over a Serial Port....1847

18 OptiCable EoC Bandwidth Configuration....1859

18.1 Configuring Example of EoC Services (OLTs Use GPON Access)....1860

19 IPv6 Configuration....1871

19.1 IPv6 Networking....1872
19.2 Configuration Difference Between IPv6 and IPv4....1874
19.2.1 Configuration Differences Between IPv6 and IPv4 on the OLT....1874
19.2.2 Configuration Differences Between IPv6 and IPv4 on the ONU....1878
19.2.3 Configuration Difference Between IPv6 and IPv4 on the ONT....1883
19.3 Configuring IPv6 Services in the FTTB/C (No HGWs) Scenario....1884
19.3.1 Application Scenarios....1884
19.3.2 Data Planning....1885
19.3.3 Configuration Procedure....1887
19.3.4 Configuration Example....1889
19.4 Configuring IPv6 Services in the FTTB+HGW Scenario....1897
19.4.1 Application Scenario....1897

Copyright © Huawei Technologies Co., Ltd.

19.4.2 Data Planning....1898
19.4.3 Configuration Procedure....1902
19.4.4 Configuration Example....1904
19.5 Configuring IPv6 Services in the FTTH (Bridging ONT) Scenario....1915
19.5.1 Application Scenarios....1915
19.5.2 Data Planning....1916
19.5.3 Configuration Procedure....1919
19.5.4 Configuration Example....1920
19.6 Configuring IPv6 Services in the FTTH (Gateway ONT) Scenario....1934
19.6.1 Application Scenarios....1934
19.6.2 Data Plan....1935
19.6.3 Configuration Procedure....1938
19.6.4 Configuration Example....1939

Copyright © Huawei Technologies Co., Ltd.

1 Commissioning

About This Chapter

This document describes the commissioning of the basic functions provided by the device in terms of hardware, software, interconnection, and maintenance and management to ensure that the device runs in a stable and reliable state.

1.1 Commissioning Introduction
The topic describes the commissioning definition and procedure.

1.2 Commissioning Preparations
This topic describes the hardware, software, and tool preparations for the commissioning.

1.3 Stand-Alone Commissioning
After the hardware installation, a stand-alone MA5600T/MA5603T/MA5608T should be commissioned to ensure that the stand-alone MA5600T/MA5603T/MA5608T works in the normal state. The following recommended commissioning tasks and sequences are for reference only. Different offices have different conditions; therefore, it is recommended that customers, with the assistance of Huawei engineers, modify commissioning tasks according to actual requirements.

1.4 Interconnection Commissioning
The MA5600T/MA5603T/MA5608T provides multiple interfaces for interconnection. This topic describes the interconnection commissioning of the MA5600T/MA5603T/MA5608T. The following recommended commissioning tasks and sequences are for reference only. Different offices have different conditions; therefore, it is recommended that customers, with the assistance of Huawei engineers, modify commissioning tasks according to actual requirements.

1.5 Maintenance and Management Commissioning
To ensure the stability of the MA5600T/MA5603T/MA5608T, you need to verify the maintainability and reliability of the device after completing the stand-alone commissioning and interconnection commissioning.

1.6 Supplementary Information
This topic provides the commissioning supplementary information, including script making, transmission mode setting, and default software settings.

Copyright © Huawei Technologies Co., Ltd.

1.1 Commissioning Introduction

The topic describes the commissioning definition and procedure.

1.1.1 Commissioning Definition

Commissioning refers to the stand-alone commissioning, the interconnection commissioning, and the maintenance and management commissioning after the hardware installation. This ensures that the device works in the normal state according to the design specifications.

1.1.2 Commissioning Procedure

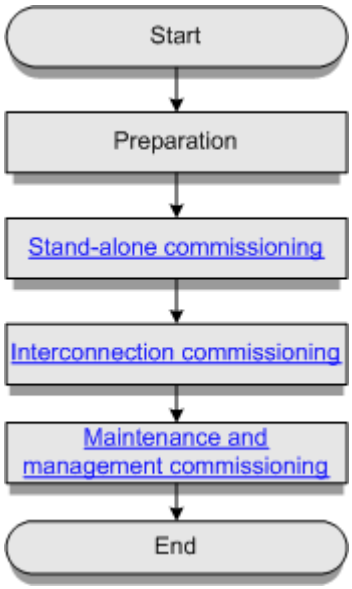
This topic describes the procedure for commissioning the device.

Flowchart

Perform the commissioning according to the flowchart.

Figure 1-1 shows the commissioning procedure.

Figure 1-1 Commissioning procedure



Commissioning Item

The commissioning items in the commissioning procedure are described as follows:

Commissioning Preparations

This topic describes the hardware, software, and tool preparations for the commissioning.

Stand-Alone Commissioning

Copyright © Huawei Technologies Co., Ltd.

After the hardware installation, a stand-alone MA5600T/MA5603T/MA5608T should be commissioned to ensure that the stand-alone MA5600T/MA5603T/MA5608T works in the normal state.

Interconnection Commissioning

The MA5600T/MA5603T/MA5608T provides multiple interfaces for interconnection. This topic describes the interconnection commissioning of the MA5600T/MA5603T/MA5608T.

Maintenance and Management Commissioning

To ensure the stability of the MA5600T/MA5603T/MA5608T, you need to verify the maintainability and reliability of the device after completing the stand-alone commissioning and interconnection commissioning.

1.2 Commissioning Preparations

This topic describes the hardware, software, and tool preparations for the commissioning.

1.2.1 Checking Hardware

This topic describes how to prepare the hardware required before the commissioning. This facilitates the subsequent commissioning.

Context

Table 1-1 lists the hardware to be checked before the commissioning.

Table 1-1 Hardware checklist

SN	Item	Description
1	Power supply and grounding	Ensure that the power cable and the grounding meet the following requirements: ● The power cable and the ground cable are connected properly and are in good contact. ● The labels of the power cable, ground cable, and power distribution switch are correct, legible and complete. ● The connectors of the external ground cables and protection ground cables of the cabinet are connected properly, without any damage. ● The power supply for the device is in the normal state.
2	Cables and connectors	Check the local maintenance serial port cable, network cable, optical fiber, subscriber cable, and connectors, and ensure that they meet the following requirements: ● The connectors are tight and firm. ● The cable jacket is intact. ● Cable labels are legible. ● Cables are bundled properly.

Copyright © Huawei Technologies Co., Ltd.

SN	Item	Description
3	Upper-layer device	Ensure that the upper-layer device meets the following requirements: ● The position of the interconnection port of the upper-layer device is correct. ● The upper-layer device works in the normal state and can be used for the commissioning.
4	Board (daughter board)	The board (daughter board) selected should meet the requirements for the external ports. **NOTE** ● Different boards (daughter boards) provide different external ports. For details about the boards and their external ports on the MA5600T/MA5603T/MA5608T, see Board Overview of the MA5600T/MA5603T/MA5608T Hardware Description. ● During the system startup, you are not allowed to install or remove any boards.

1.2.2 Preparing Software

This topic describes how to prepare the software required before the commissioning. This facilitates the subsequent commissioning.

Table 1-2 shows the software checklist before the commissioning.

Table 1-2 Software checklist

SN	Item	Description
1	Software package	Ensure that files in the software package for the commissioning are complete and the software version is correct.
2	Software commissioning tools	Ensure that all the commissioning tools are available. The common commissioning tools are as follows: ● HyperTerminal (provided by the Windows OS): used for logging in to the MA5600T/MA5603T/MA5608T through the CLI. ● TFTP, SFTP, and FTP tools: used for loading software. They can be downloaded from **http://support.huawei.com**. You are advised to use SFTP tools. ● Client software key generator Puttygen.exe, client software key convertor sshkey.exe and SSH client software putty.exe: used for logging in to the MA5600T/MA5603T/MA5608T through the SSH.

Copyright © Huawei Technologies Co., Ltd.

1.2.3 Preparing Tools

This topic describes how to prepare the tools required before the commissioning. This facilitates the subsequent commissioning.

Table 1-3 lists the tools to be prepared for the commissioning.

Table 1-3 Tool checklist

SN	Item	Description	Remarks
1	Cables	One RS-232 serial port cable (One end with an RJ-45 connector used to connect to the board and the other end with a DB-9 or DB-25 female connector used to connect to the maintenance terminal)	Used to connect the maintenance terminal to the MA5600T/MA5603T/ MA5608T for maintenance through the serial port.
		One crossover cable	Used to connect the maintenance terminal to the MA5600T/MA5603T/ MA5608T for maintenance through telnet.
		Some optical fibers and patch cords with different connectors	Used for the upstream transmission and optical power test.
2	Maintenance terminal	One maintenance terminal configured with a HyperTerminal application, such as a laptop	Used to log in to the MA5600T/MA5603T/ MA5608T to commission the MA5600T/MA5603T/ MA5608T.
3	Auxiliary device and meter	One optical power meter	Used to test the mean launched power and the input optical power of an optical port.
		One optical attenuator	Used to attenuate the input optical signal. It is used to protect the optical port from being damaged by intense optical signals during the device commissioning.
		One multimeter	Used to measure the voltage, resistance and current intensity during the power commissioning.

Copyright © Huawei Technologies Co., Ltd.

SN	Item	Description	Remarks
		One optical multiplexer/demultiplexer	Used to test the input optical power of a single-fiber bi-directional optical port. It is a meter with the multiplexing and demultiplexing functions.
		One data network performance analyzer	Used to test the input optical power. It is used to transmit data to simulate the networking environment.

1.2.4 Planning Data

This topic describes the information to be collected about the hardware configuration, networking, and data plan before the commissioning based on the engineering document. This facilitates the data configuration.

Table 1-4 lists the data collected for the commissioning.

Table 1-4 Data checklist

SN	Item	Description
1	Hardware configuration	This includes but is not limited to the following: ● Types and slot distribution of the control board and service boards ● Types and physical positions of the upstream ports and the service ports
2	Networking and data plan	This includes but is not limited to the following: ● Networking mode ● IP address assignment ● VLAN planning
3	DIP Switches configuration **NOTE** Only the MA5600T supports this operation.	● For details about the default settings of DIP switches on the ESC board on the MA5600T, see **1.3.1.1 Checking the Settings of DIP Switches on the H801ESC Board**. ● For details about the default settings of DIP switches on the fan monitoring board on the MA5600T, see **1.3.1.2 Checking the Settings of DIP Switches on the Fan Monitoring Board**.

Copyright © Huawei Technologies Co., Ltd.

NOTE

- A commissioning script can be made based on the actual networking and the data plan. For how to make a script, see **1.6.1 Script Making**.
- For details about the default settings of the main software on the MA5600T/MA5603T/MA5608T, see **1.6.3 Software Package Settings**.

1.3 Stand-Alone Commissioning

After the hardware installation, a stand-alone MA5600T/MA5603T/MA5608T should be commissioned to ensure that the stand-alone MA5600T/MA5603T/MA5608T works in the normal state. The following recommended commissioning tasks and sequences are for reference only. Different offices have different conditions; therefore, it is recommended that customers, with the assistance of Huawei engineers, modify commissioning tasks according to actual requirements.

1.3.1 Checking the Settings of DIP Switches

This topic describes how to check the settings of the DIP switches on the environment monitoring board (ESC board) and the fan monitoring board. This ensures the consistency between the settings of DIP switches and the application of DIP switches.

1.3.1.1 Checking the Settings of DIP Switches on the H801ESC Board

This topic describes how to check the settings of DIP switches on the H801ESC board. Checking the settings of DIP switches helps ensure that the settings meets actual requirements.

Prerequisites

The device must be powered off.

Description of DIP Switches

The H801ESCA board resides in the I-type PDU and provides two DIP switches, namely, S5 and S6. **Figure 1-2** shows the layout of the DIP switches on the H801ESCA board.

Figure 1-2 Layout of the DIP switches (in default settings) on the H801ESCA board

Table 1-5 describes the usage of DIP switches S5 and S6.

Copyright © Huawei Technologies Co., Ltd.

Table 1-5 Usage of the DIP switches

Electric Switch	Usage
S5-1	Used to set the external sensor type of JTA1-JTA4. For detailed information, see **Table 1-6**. ● ON: The external sensors are of the current type. ● OFF: The external sensors are of the voltage type.
S5-2	
S5-3	
S5-4	
S6-1	Used to set the sub-node ID. This value must correspond with the configured ESC sub-node ID in the system and cannot be identical to the address value of the sub-node. Such restrictions ensure that the H801ESC board can communicate with the control board. For detailed information, see **Table 1-7**. ● ON: The mapping address bit is 0. ● OFF: The mapping address bit is 1.
S6-2	
S6-3	
S6-4	
S6-5	
S6-6	Reserved.
S6-7	
S6-8	Used to set the baud rate of the communication between the H801ESCA board and the control board. ● ON: The baud rate is 19200 bit/s (default). ● OFF: The baud rate is 9600 bit/s.

Table 1-6 describes the mapping between S5-1 to S5-4 and sensor ports.

Table 1-6 Mapping between S5-1 to S5-4 and sensor ports

Electric Switch	OFF	ON
S5-1	The external sensor of JTA1 is of the voltage type.	The external sensor of JTA1 is of the current type.
S5-2	The external sensor of JTA2 is of the voltage type.	The external sensor of JTA2 is of the current type.
S5-3	The external sensor of JTA3 is of the voltage type.	The external sensor of JTA3 is of the current type.
S5-4	The external sensor of JTA4 is of the voltage type.	The external sensor of JTA4 is of the current type.

S6-1 to S6-5 are used to set the sub-node IDs of the H801ESC board. **Table 1-7** lists the mapping between S6-1 to S6-5 and sub-node IDs.

Copyright © Huawei Technologies Co., Ltd.

Table 1-7 Mapping between S6-1 to S6-5 and sub-node IDs

S6-5	S6-4	S6-3	S6-2	S6-1	Address Value of Sub-nodes
0	0	0	0	0	00000 (0)
0	0	0	0	1	00001(1)
0	0	0	1	0	00010(2)
0	0	0	1	1	00011(3)
0	0	1	0	0	00100(4)
0	0	1	0	1	00101(5)
0	0	1	1	0	00110(6)
0	0	1	1	1	00111(7)
0	1	0	0	0	01000(8)
0	1	0	0	1	01001(9)
0	1	0	1	0	01010(10)
0	1	0	1	1	01011(11)
0	1	1	0	0	01100(12)
0	1	1	0	1	01101(13)
0	1	1	1	0	01110(14)
0	1	1	1	1	01111(15) (default)
1	0	0	0	0	10000(16)
1	0	0	0	1	10001(17)
1	0	0	1	0	10010(18)
1	0	0	1	1	10011(19)
1	0	1	0	0	10100(20)
1	0	1	0	1	10101(21)
1	0	1	1	0	10110(22)
1	0	1	1	1	10111(23)
1	1	0	0	0	11000(24)
1	1	0	0	1	11001(25)
1	1	0	1	0	11010(26)

Copyright © Huawei Technologies Co., Ltd.

S6-5	S6-4	S6-3	S6-2	S6-1	Address Value of Sub-nodes
1	1	0	1	1	11011(27)
1	1	1	0	0	11100(28)
1	1	1	0	1	11101(29)
1	1	1	1	0	11110(30) is used by the ESC board, and the H801ESC board cannot be set to this value.
1	1	1	1	1	11111(31)

Procedure

Step 1 Remove the cable connector if the H801ESC board is connected to an environment monitoring cable.

Step 2 Loosen the screws on the H801ESC board anticlockwise by using the Phillips screwdriver, as shown in (1) of **Figure 1-3**.

Figure 1-3 Removing the H801ESC board

Step 3 Hold the ejector lever of the front panel and remove the H801ESC board from the PDU, as shown in (2) of **Figure 1-3**.

Copyright © Huawei Technologies Co., Ltd.

Step 4 Check whether settings of DIP switches on the H801ESC board are consistent with the application. If the settings are inconsistent with the application, set the DIP switches again according to "Description of DIP Switches".

Step 5 Insert the H801ESC board into the PDU, as shown in (1) of **Figure 1-4**.

Figure 1-4 Inserting the H801ESC board

Step 6 Fasten the screws on the H801ESC board clockwise by using the Phillips screwdriver, as shown in (2) of **Figure 1-4**.

Step 7 Reconnect the environment monitoring cable to the H801ESC board.

----End

Result

The settings of DIP switches on the H801ESC board are consistent with the actual requirements.

1.3.1.2 Checking the Settings of DIP Switches on the Fan Monitoring Board

This topic describes how to check the settings of DIP switches on the fan monitoring board. Checking the settings of DIP switches helps ensure that the settings meet the application of DIP switches.

Prerequisites

NOTE

Do not change the DIP switch setting on the fan monitoring board of the MA5603T. The DIP switches on the fan monitoring board of the MA5608T does not support the DIP switch.

The device must be powered off.

Copyright © Huawei Technologies Co., Ltd.

Description of DIP Switches

The ESTI fan tray uses the FCBI fan monitoring board, and the 19-inch fan tray uses the FCBH fan monitoring board.

The fan monitoring board provides a set of DIP switches named SW2. **Figure 1-5** and **Figure 1-6** show the layout of the DIP switches of the ESTI and the 19-inch fan trays respectively.

Figure 1-5 Layout of the DIP switches (in default settings) of the ESTI fan tray

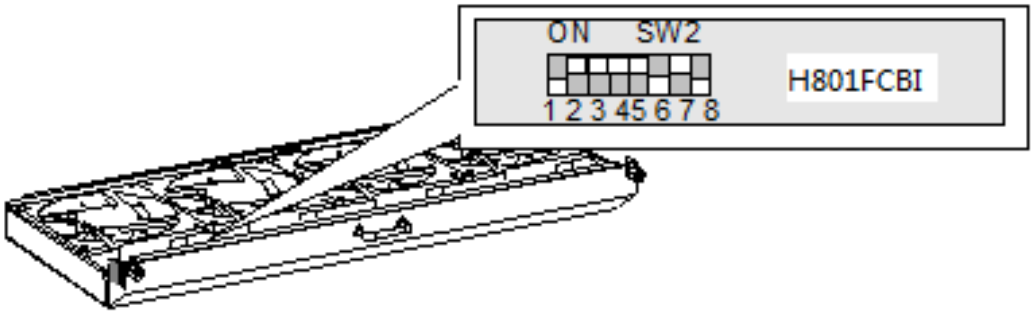


Figure 1-6 Layout of the DIP switches (in default settings) of the 19-inch fan tray

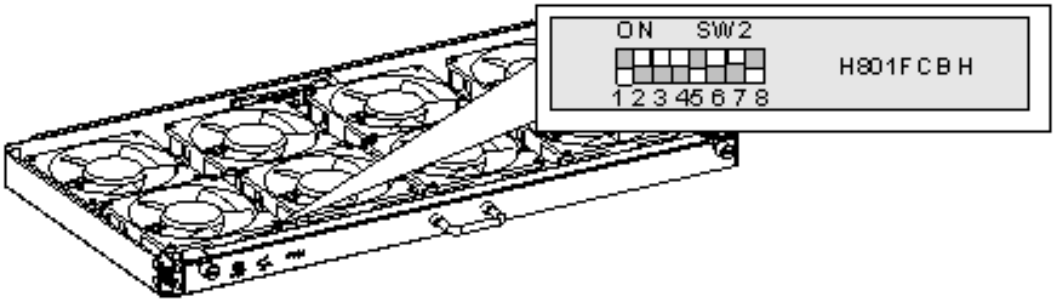


Table 1-8 lists the usage of the SW2.

Table 1-8 usage of the SW2

DIP Switch	Usage
SW2-1	Used to set the sub-node address. This value must correspond with the configured sub-node address of the fan in the system and cannot be identical to the address value of the ESC sub-node. Such restrictions ensure that the fan tray can communicate with the control board. For detailed information, see **Table 1-9**. ● ON: The mapping address bit is 0. ● OFF: The mapping address bit is 1.
SW2-2	
SW2-3	
SW2-4	Used to set the baud rate of the communication between the fan tray and the control board. ● ON: The baud rate is 19200 bit/s (default). ● OFF: The baud rate is 9600 bit/s.

Copyright © Huawei Technologies Co., Ltd.

DIP Switch	Usage
SW2-5	Used to set the number of fans. This value must correspond with the system data configuration. For detailed information, see **Table 1-10**.
SW2-6	
SW2-7	Used to set the fan speed adjustment mode. This value must correspond with the system data configuration. For detailed information, see **Table 1-11**.
SW2-8	

Table 1-9, **Table 1-10**, and **Table 1-11** list the settings of each DIP switch of SW2.

Table 1-9 Settings of SW2-1 to SW2-3

SW2-3	SW2-2	SW2-1	Address Value
ON	ON	ON	000(0)
ON	ON	OFF	001(1) (default setting)
ON	OFF	ON	010(2)
ON	OFF	OFF	011(3)
OFF	ON	ON	100(4)
OFF	ON	OFF	101(5)
OFF	OFF	ON	110(6)
OFF	OFF	OFF	111(7)

Table 1-10 Settings of SW2-5 and SW2-6

SW2-6	SW2-5	Quantity of Fans	Remarks
ON	ON	6	-
ON	OFF	8	The unique and default setting of the 19-inch fan tray
OFF	ON	4	The unique and default setting of the ETSI fan tray
OFF	OFF	10	-

Copyright © Huawei Technologies Co., Ltd.

Table 1-11 Settings of SW2-7 and SW2-8

SW2-8	SW2-7	Speed Adjustment Mode	Speed Adjustment Policy	Remarks
ON	ON	Measure the temperature at the air intake vent (reserved)	Policy 1 ● If the temperature is lower than 25°C, the fans rotate at 50% of the full speed. ● If the temperature ranges from 25°C to 35°C, the fans rotate at 50% to 100% of the full speed. ● If the temperature is higher than 35°C, the fans rotate at full speed.	-
ON	OFF	Measure the temperature at the air exhaust vent	Policy 2 ● If the temperature is lower than 55°C, the fans rotate at 50% of the full speed. ● If the temperature ranges from 55°C to 65°C, the fans rotate at 50% to 100% of the full speed. ● If the temperature is higher than 65°C, the fans rotate at the full speed.	-
OFF	ON	Measure the temperature at the air intake vent	Policy 3 ● If the temperature is lower than 30°C, the fans rotate at 50% of the full speed. ● If the temperature ranges from 30°C to 50°C, the fans rotate at 50% to 100% of the full speed. ● If the temperature is higher than 50°C, the fans rotate at full speed.	The ESTI and the 19-inch fan trays support only policy 3. Therefore, only this setting can be adopted.

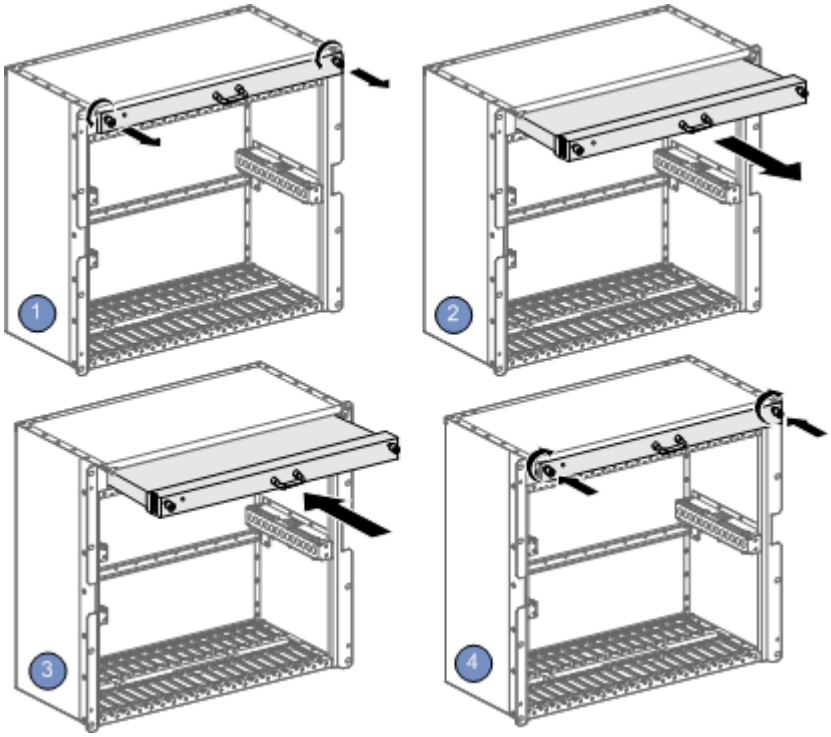
Copyright © Huawei Technologies Co., Ltd.

SW2-8	SW2-7	Speed Adjustment Mode	Speed Adjustment Policy	Remarks
OFF	OFF	Stop fan rotating and measure the temperature at the air intake vent	Policy 4 ● If the temperature is lower than 15°C, the fans stop rotating. ● If the temperature ranges from 15°C to 45°C, the fans rotate at 50% of the full speed. ● If the temperature ranges from 45°C to 65°C, the fans rotate at 50% to 100% of the full speed. ● If the temperature is higher than 65°C, the fans rotate at full speed.	-

Procedure

Step 1 Loosen the screws on the front panel of the fan tray anticlockwise by using the Phillips screwdriver, as shown in (1) of **Figure 1-7**.

Figure 1-7 Removing/Inserting the fan tray



Copyright © Huawei Technologies Co., Ltd.

Step 2 Hold the ejector lever of the fan tray and remove the fan tray from the service shelf, as shown in (2) of **Figure 1-7**.

Step 3 Check whether the settings of DIP switches on the fan monitoring board are consistent with the application. If settings of DIP switches on the fan monitoring board are not consistent with the application, set the DIP switches again according to "Description of DIP Switches".

Step 4 Insert the fan tray into the slot, as shown in (3) of **Figure 1-7**.

Step 5 Use the Phillips screwdriver to fasten the panel screws clockwise on the fan tray, as shown in (4) of the **Figure 1-7**.

----End

Result

The settings of DIP switches on the fan monitoring board are consistent with the application.

1.3.2 Powering On the Device

This topic describes how to power on the device to ensure that all the boards can be normally powered on.

Prerequisites

The after-installation check and the power-on check must be performed on the device.

Context

NOTICE

Inserting or removing boards is prohibited during startup.

Procedure

- There are two kinds of devices: the indoor device and the outdoor device.
  - Powering on the indoor device
    1. Connect the input power supply of the DC PDU.
    2. Turn on the output control switch of the DC PDU.
  - Powering on the outdoor device
    1. Connect the input power supply of the AC PDU.
    2. Turn on the output control switch of the AC PDU.
    3. Turn on the output control switch of the power system.
    4. Turn on the output control switch of the DC PDU.

----End

Copyright © Huawei Technologies Co., Ltd.

Result

The device can be normally powered on, and the STATUS indicator on the fan tray is on for 1s and off for 1s repeatedly, and so is the RUN ALM indicator on the board.

1.3.3 Commissioning the Power Supply System

This topic describes how to commission the power supply to ensure the reliable and stable power supply provided for the device.

1.3.3.1 Checking the Power Supply of the DC PDU

This topic describes how to verify that either of the two independent power supplies can supply power to the cabinet.

Prerequisites

- Only the MA5600T supports this operation.
- The two independent power supplies of the DC power distribution unit (PDU) supply power to the cabinet concurrently.

Procedure

Step 1 Disconnect the first power supply, and check the power supply of the cabinet.

Step 2 Restore the first power supply to power the cabinet.

Step 3 Disconnect the second power supply, and check the power supply of the cabinet.

Step 4 Restore the second power supply to power the cabinet.

----End

Result

After either of the two independent power supplies is disconnected, the power supply of the cabinet is in the normal state, and the power supply of the boards is not affected, that is, the RUN LED on the board is on for 1s and off for 1s repeatedly.

1.3.3.2 Checking the Power Supply of the Power Board

This topic describes how to check the redundancy backup function of the power boards.

Prerequisites

The two power boards configured must work in the normal state.

Context

In the normal state, the two power boards work in the load balancing mode and provide power for all the service boards in the shelf. When one power board is faulty, the other power board provides power for all the service boards in the shelf.

When checking the power supply of the power board, pay attention to the following points:

Copyright © Huawei Technologies Co., Ltd.

- Wear an ESD wrist strap during the operation.
- Turn off the -48 V input switch on the PDU that corresponds to the power board before replacing the board. In addition, when the board is powered on, do not remove or insert the power connector.
- If one power board is faulty, replace the board in time to prevent the shelf from working for a long time when only one power board supplies power.

Procedure

Step 1 Turn off the switch on the PDU that corresponds to one power board, and check the power supply for the service board.

Step 2 Turn on the switch again.

Step 3 Repeat steps 1 and 2 to check the other power board.

----End

Result

The boards in the shelf work in the normal state after the switch on the PDU that corresponds to either power board is turned off, that is, the RUN LED on the board is on for 1s and off for 1s repeatedly.

1.3.4 Configuring the Maintenance Terminal

During the commissioning, you need to maintain the device through the maintenance terminal. This topic describes how to start the maintenance terminal and configure the IP address of the maintenance terminal to meet the commissioning requirements.

Context

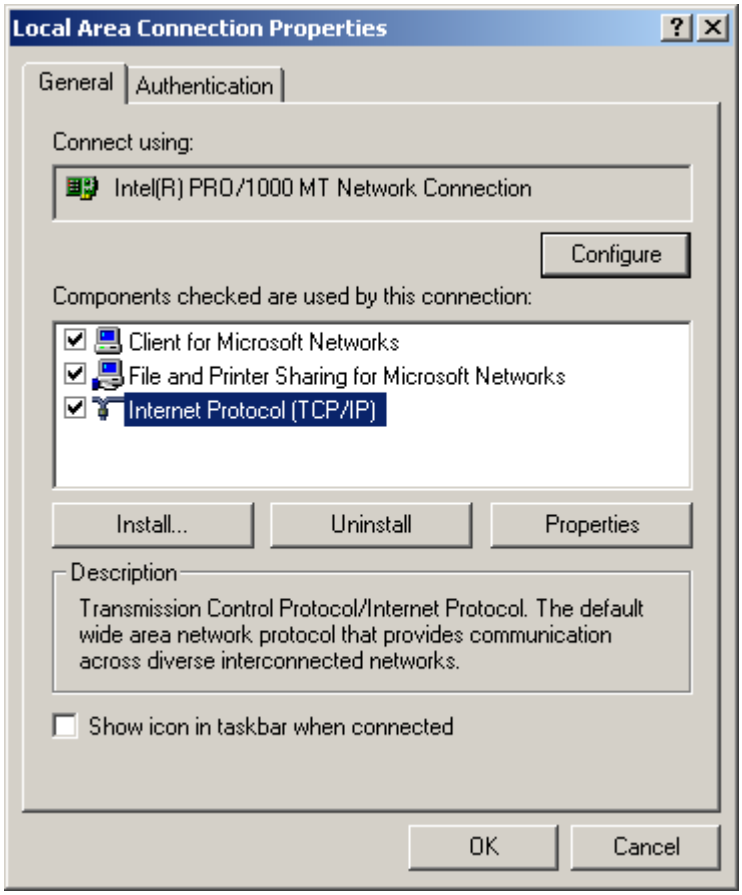
A maintenance terminal is usually a laptop installed with a HyperTerminal application.

Procedure

- Starting the Maintenance Terminal.
  1. Power on the maintenance terminal. The Windows OS starts automatically, and the **Log In** dialog box is displayed.
  2. Power on the maintenance terminal. The Windows OS starts automatically, and the **Log In** dialog box is displayed.
  3. Click **OK** to enter the Windows OS.
- Configuring the IP address of the maintenance terminal to ensure that you can log in to the MA5600T/MA5603T/MA5608T in the telnet or SSH mode through the maintenance terminal. You are advised to use SSH mode.
  1. Right-click **My Network Places** and choose **Properties**. The **Network Connections** window is displayed.
  2. In the **Network Connections** window, right-click **Local Area Connection**, and choose **Properties**. The **Local Area Connection Properties** dialog box is displayed.
  3. Click the **General** tab, and then select **Internet Protocol (TCP/IP)** in **Components checked are used by this connection**, as shown in the following figure.

Copyright © Huawei Technologies Co., Ltd.

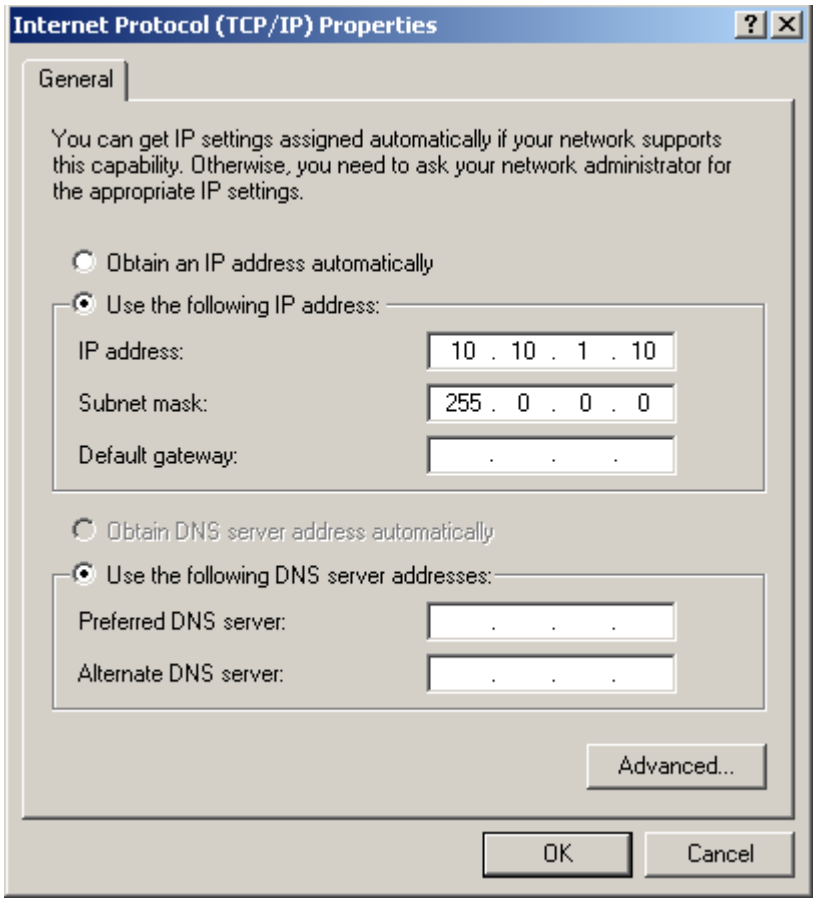
Figure 1-8 Configure the local area connection properties



4. Click **Properties** to display the **Internet Protocol (TCP/IP) Properties** dialog box.
5. Click **General**, and then select **Use the following IP address:** to configure the IP address and the subnet mask, as shown in the following figure.

Copyright © Huawei Technologies Co., Ltd.

Figure 1-9 Configure the IP address and the subnet mask



NOTE

The IP address of the maintenance terminal and the IP address of the maintenance Ethernet port of the device must be in the same network segment.

6. Click **OK** to return to the **Local Area Connection Properties** dialog box.
7. Click **OK**.

----End

Result

The IP address of the maintenance terminal and the IP address of the maintenance Ethernet port of the device are in the same network segment.

NOTE

By default, the IP address of the maintenance network port (ETH port on the control board) is 10.11.104.2, and the subnet mask is 255.255.255.0.

1.3.5 Logging In to the System

You must log in to the MA5600T/MA5603T/MA5608T before commissioning the MA5600T/MA5603T/MA5608T through the maintenance terminal. The following describes three login modes, namely, local serial port mode, telnet mode, and SSH mode. SSH with high priority is recommended.

Copyright © Huawei Technologies Co., Ltd.

1.3.5.1 Login Through the Local Serial Port

When you need to maintain and manage the MA5600T/MA5603T/MA5608T locally, you can log in to the system through the local serial port.

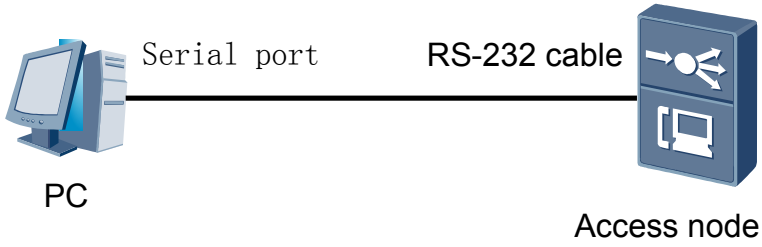
Prerequisites

- A maintenance terminal (generally a laptop configured with a HyperTerminal application) must be available.
- An RS-232 serial port cable (one end with an RJ45 connector and the other end with a DB-9 or DB-25 female connector) must be available.

Networking

Figure 1-10 shows the networking for logging in to the MA5600T/MA5603T/MA5608T through the local serial port.

Figure 1-10 Logging in to the MA5600T/MA5603T/MA5608T through the local serial port

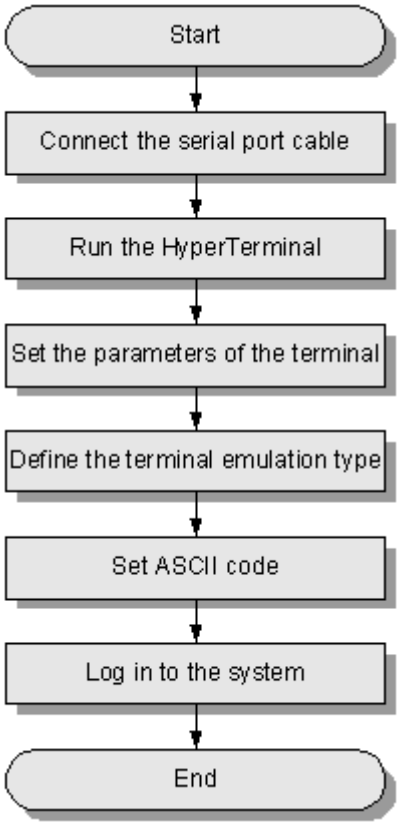


Flowchart

Figure 1-11 shows the flowchart for logging in to the system through the local serial port.

Copyright © Huawei Technologies Co., Ltd.

Figure 1-11 Flowchart for logging in to the system through the local serial port



Procedure

Step 1 Connect the serial port cable.

Use an RS-232 serial port cable to connect a serial port of the PC to the CON port of the SCU control board, as shown in **Figure 1-10**.

Step 2 Set the HyperTerminal communication parameters.

NOTE

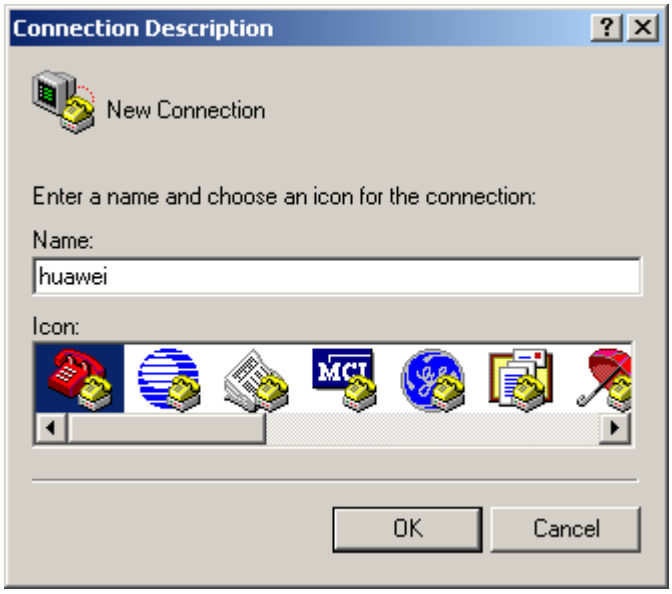
This section uses the HyperTerminal of the Windows XP OS as an example. If other OSs, such as Windows 7, are not equipped with the HyperTerminal, download the HyperTerminal.

The following section considers the typical mode in Windows as an example to describe how to log in to the system in the local serial port mode. Other modes are not described here.

1. Set up a connection.

   Click **Start**. Choose **All Programs** > **Accessories** > **Communications** > **Hyper Terminal** to display the **Connection Description** dialog box. Input the connection name, and click **OK**, as shown in the following figure.

Copyright © Huawei Technologies Co., Ltd.

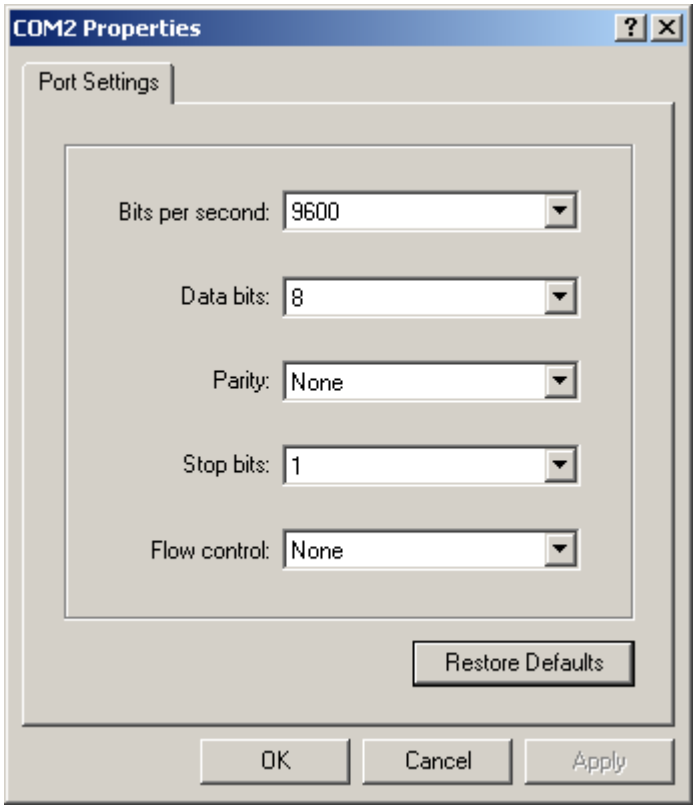


2. Set the serial port.

   Select the serial port that is connected to the MA5600T/MA5603T/MA5608T. You can select **COM1** or **COM2** (here, use **COM2** as an example), and click **OK**, as shown in the following figure.

3. Set the HyperTerminal communication parameters. For details, see the following figure.

Copyright © Huawei Technologies Co., Ltd.



NOTE

- The baud rate of the HyperTerminal must be the same as the baud rate of the serial port on the MA5600T/MA5603T/MA5608T. By default, the baud rate of the serial port is 9600 bit/s.
- If illegible characters are displayed on the HyperTerminal interface after you log in to the system, it is generally because the baud rate of the HyperTerminal is different from the baud rate of the MA5600T/MA5603T/MA5608T. In this case, set the consistent baud rate for the HyperTerminal to log in to the system. The system supports the baud rates of 9600 bit/s, 19200 bit/s, 38400 bit/s, 57600 bit/s, and 115200 bit/s.

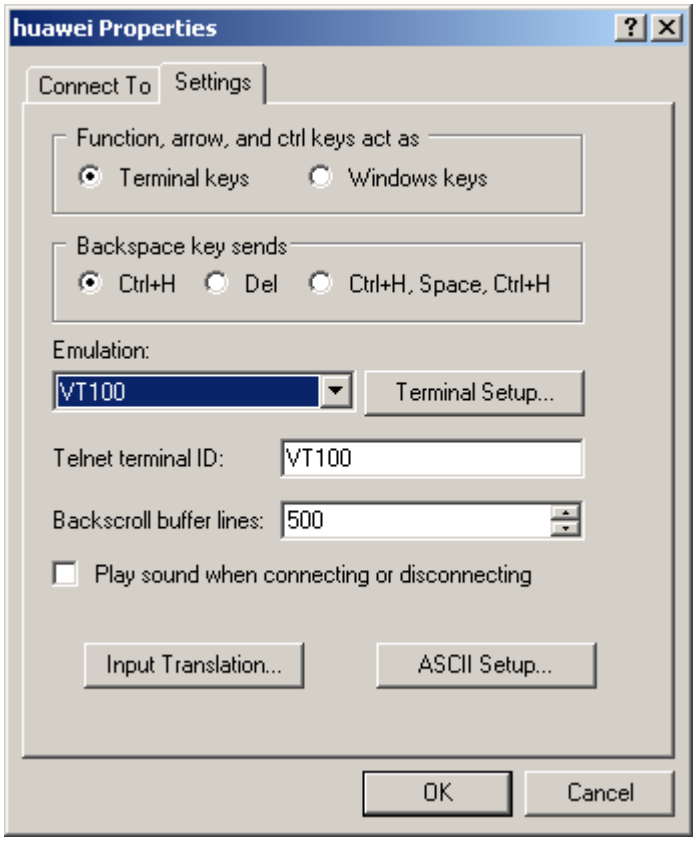
4. Click **OK** to display the HyperTerminal interface.

Step 3 (Optional) Set the properties of the HyperTerminal.

1. Set the emulation type of the HyperTerminal.

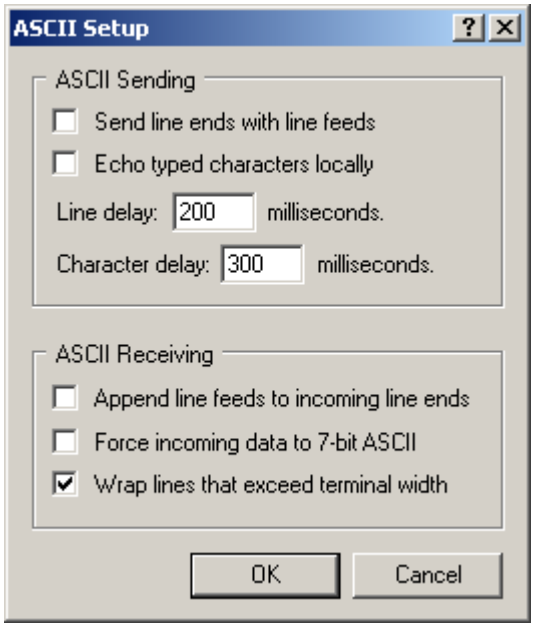
   Choose **File** > **Properties** on the HyperTerminal interface. In the dialog box that is displayed, click the **Settings** tab, and set **Emulation** to **VT100** or **Auto Detect**, as shown in the following figure. It is **Auto Detect** by default.

Copyright © Huawei Technologies Co., Ltd.



2. Set the line delay and the character delay of the ASCII code.

   Click **ASCII Setup**. In the dialog box that is displayed, set **line delay** to **200** and **Character delay** to **200**, and then click **OK**, as shown in the following figure. By default, **Line delay** is **0**, and **Character delay** is **0**.



Copyright © Huawei Technologies Co., Ltd.

NOTE

When you paste a text to the HyperTerminal, the character delay controls the character transmit speed, and the line delay controls the interval of transmitting every line. If a delay is very short, loss of characters occurs. When the pasted text is displayed abnormally, modify the delay.

----End

Result

On the Hyper Terminal interface, press **Enter**, and the system prompts you to input the user name. Input the user name and the password for user registration (by default, the super user name is **root** and the password is **admin**), and wait until the CLI prompt character is displayed.

NOTE

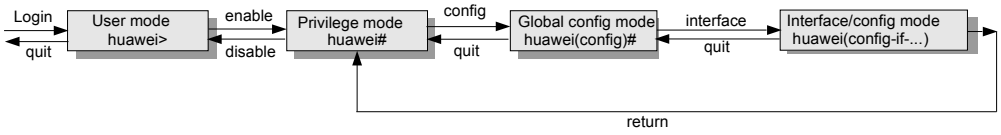
To improve the system security, please modify your password after first login. You can run the **terminal user password** command to modify your password.

If the login fails, click and then click on the operation interface. If the login still fails, return to step 1 to check the parameter settings and the physical connections, and then try again.

Follow-up Procedure

- You can run the **idle-timeout** command to set the terminal timeout time. if you do not input commands within the specified timeout time, the system disconnects the terminal. By default, the terminal timeout time is set to 5 minutes. If you do not run any commands within 5 minutes, the system disconnects with the terminal. To perform any operation, you must have to log in to the system again.
- In the commissioning procedure, you must use the command, It is recommended that you know well the command modes first.**Figure 1-12** shows how to switch command modes.

Figure 1-12



1.3.5.2 Login Through Telnet (Outband Management)

This topic describes how to log in to the MA5600T/MA5603T/MA5608T using the local maintenance Ethernet port (outband management port) in the telnet mode to maintain and manage the MA5600T/MA5603T/MA5608T. You are advised to use SSH mode.

Prerequisites

Engineers are logged in to the MA5600T/MA5603T/MA5608T by using the local serial port or the ETH port.

NOTE

The default IP address of the maintenance Ethernet port (ETH port on the control board) is 10.11.104.2, and the subnet mask is 255.255.255.0.

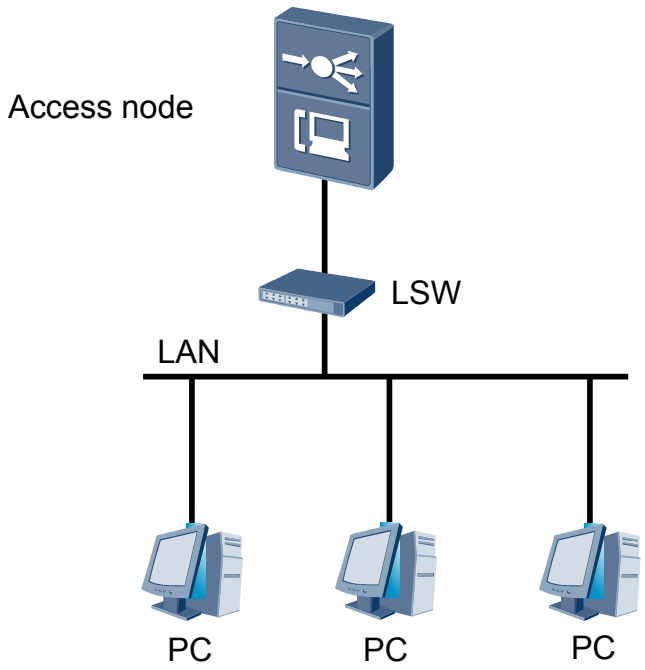
Copyright © Huawei Technologies Co., Ltd.

- For details about how to log in to the MA5600T/MA5603T/MA5608T by using the local serial port, see **1.3.5.1 Login Through the Local Serial Port**.
- For details about how to log in to the MA5600T/MA5603T/MA5608T by using the ETH port, see the following:
  - Configure the IP address of the PC that is used for logging in to the MA5600T/MA5603T/MA5608T. This IP address is on the same subnet as the IP address of the maintenance Ethernet port but is not the IP address of the maintenance Ethernet port. For example, configure the IP address to 10.11.104.6.
  - After logging in to the MA5600T/MA5603T/MA5608T, run the **ip address** command to change the IP address of the device to 10.50.1.10/24.
  - Change the IP address of the PC to be on the same subnet as the IP address of the maintenance Ethernet port but is not the IP address of the maintenance Ethernet port. For example, change the IP address of the device to 10.50.1.11/24.

Networking

Figure 1-13 shows an example network for outband management through telnet in a LAN, and **Figure 1-14** shows an example network for outband management through telnet in a WAN.

Figure 1-13 Example network for outband management through telnet in a LAN

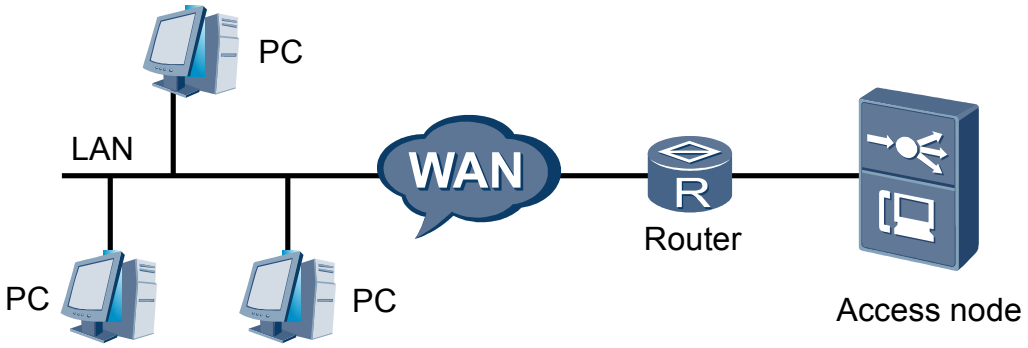


NOTE

The MA5600T/MA5603T/MA5608T is connected to the LAN using the straight using cable, and the IP address of the maintenance Ethernet port of the MA5600T/MA5603T/MA5608T is in the same network segment as the IP address of the maintenance terminal. Alternatively, the Ethernet port of the maintenance terminal can be directly connected to the maintenance Ethernet port of the MA5600T/MA5603T/MA5608T to manage the MA5600T/MA5603T/MA5608T in the outband management mode. In such a condition, if the MA5600T/MA5603T/MA5608T uses SCUL/SCUB control board, and the peer device does not support the cable autosensing function, a crossover cable must be used.

Copyright © Huawei Technologies Co., Ltd.

Figure 1-14 Network example for outband management through telnet in a WAN



Data Plan

Table 1-12 and Table 1-13 provide the data plan for the outband management through telnet in a LAN and in a WAN respectively.

Table 1-12 Data plan for the outband management through telnet in a LAN

Item	Data
Maintenance Ethernet port of the MA5600T/ MA5603T/MA5608T	IP address: 10.50.1.10/24 **NOTE** By default, the IP address of the maintenance Ethernet port (ETH port on the control board) is 10.11.104.2, and the subnet mask is 255.255.255.0.
Maintenance terminal	IP address: 10.50.1.20/24 (in the same subnet as the IP address of the maintenance Ethernet port)

Table 1-13 Data plan for the outband management through telnet in a WAN

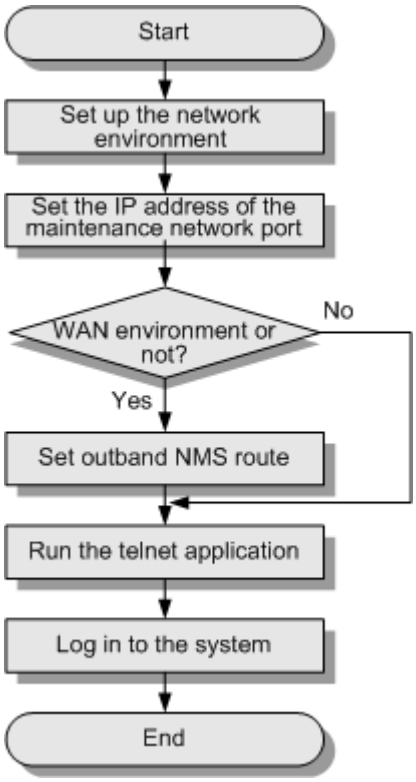
Item	Data
Maintenance Ethernet port of the MA5600T/ MA5603T/MA5608T	IP address: 10.50.1.10/24 **NOTE** By default, the IP address of the maintenance Ethernet port (ETH port on the control board) is 10.11.104.2, and the subnet mask is 255.255.255.0.
Maintenance terminal	IP address: 10.10.1.10/24
Router port connecting to the MA5600T/ MA5603T/MA5608T	IP address: 10.50.1.1/24

Copyright © Huawei Technologies Co., Ltd.

Flowchart

Figure 1-15 shows the flowchart for logging in to the MA5600T/MA5603T/MA5608T through telnet (outband management).

Figure 1-15 Flowchart for logging in to the MA5600T/MA5603T/MA5608T through telnet (outband management)



Procedure

Step 1 Set up the network environment.

- If you log in to the MA5600T/MA5603T/MA5608T in the LAN outband management mode through telnet, set up a network environment according to Figure 1-13.
- If you log in to the MA5600T/MA5603T/MA5608T in the MAN outband management mode through telnet, set up a network environment according to Figure 1-14.

Step 2 Configure the IP address of the maintenance Ethernet port.

In the MEth mode, run the **ip address** command to configure the IP address of the maintenance Ethernet port.

```
huawei(config)#interface meth 0
huawei(config-if-meth0)#ip address 10.50.1.10 24
```

Step 3 Add a route for the outband management.

- If the network environment is set up as shown in Figure 1-13, you need not add a route.

Copyright © Huawei Technologies Co., Ltd.

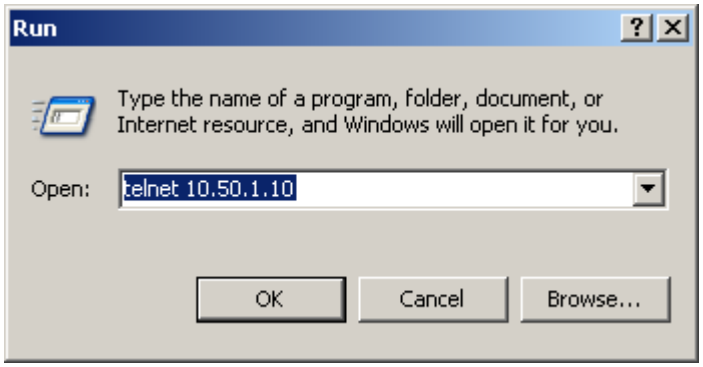
- If the network environment is set up as shown in **Figure 1-14**, run the **ip route-static** command to add a route from the maintenance Ethernet port of the MA5600T/MA5603T/MA5608T to the maintenance terminal.

```
huawei(config-if-meth0)#quit
huawei(config)#ip route-static 10.10.1.0 24 10.50.1.1
```

Step 4 Run the telnet application.

On the maintenance terminal, choose **Start** > **Run**. On the **Run** window, input "telnet 10.50.1.10" in the **Open** field as shown in **Figure 1-16** (considering the Windows OS as an example), and click **OK**. Then, the telnet dialog box is displayed.

Figure 1-16 Running the telnet application



Step 5 Log in to the system.

In the telnet dialog box, input the user name and the password. By default, the user name is **root**, and the password is **admin**. When the login is successful, the system displays the following information:

```
>>User name:root
>>User password:admin

 Huawei Integrated Access SoftwareMA5600T/MA5603T/MA5608T.
  Copyright(C) Huawei Technologies Co., Ltd. 2002-2012. All rights reserved.

  ------------------------------------------------------------------------------
  User last login information:
  ------------------------------------------------------------------------------
  Access Type : Telnet
  IP-Address  : 10.10.10.122
  Login  Time : 2011-03-29 16:03:20+08:00
  Logout Time : 2011-03-29 16:08:40+08:00
  ------------------------------------------------------------------------------
  ------------------------------------------------------------------------------
  User fail login information:
  ------------------------------------------------------------------------------
  Last Access Type    : Telnet
  Last IP-Address     : 10.10.10.74
  Last Login Time     : 2011-03-29 16:11:10+08:00
  Login Failure Times : 2
  ------------------------------------------------------------------------------
  ------------------------------------------------------------------------------
  All user fail login information:
  ------------------------------------------------------------------------------
  Access Type IP-Address           Time                          Login Times
```


Copyright © Huawei Technologies Co., Ltd.

```
------------------------------------------------------------------------------
Telnet      10.10.10.74          2011-03-29 16:11:10+08:00              1
Telnet      10.10.10.122         2011-03-29 15:37:05+08:00              3
Telnet      10.10.10.193         2011-03-25 18:19:04+08:00              1
------------------------------------------------------------------------------
```

The following table describes the parameters in response to this login.

Parameter	Description
User name	Indicates the user name.
User password	Indicates the user password that is not displayed on the maintenance terminal.
User last login information	Indicates the information about the latest successful login.
Access Type	Indicates the access type of the latest successful login.
IP-Address	Indicates the IP address of the latest successful login.
Login Time	Indicates the time of the latest successful login.
Logout Time	Indicates the time of the latest successful logout. If the user does not log out, it displays as "--".
User fail login information	Indicates the information about the failed login.
Last Access Type	Indicates the access type of the latest failed login.
Last IP-Address	Indicates the IP address of the latest failed login.
Last Login Time	Indicates the time of the latest failed login.
Login Failure Times	Indicates the failed login times. It is the times of login failures between two login successes, but not the accumulative login failures.
All user fail login information	Indicates the information about failed login of all users, which can be viewed only by user root or security administrator.
Access Type	Indicates the access type of the login.
IP-Address	Indicates the IP address of the login.
Time	Indicates the time of the login.
Login Times	Indicates the login times.

----End

Result

After logging in to the system, you can maintain and manage the MA5600T/MA5603T/MA5608T.

NOTE

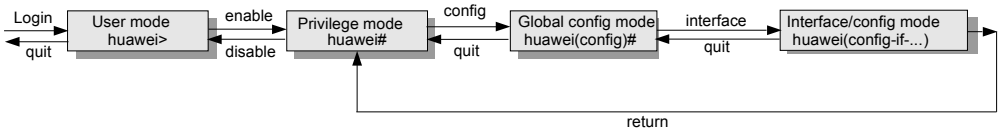
To improve the system security, please modify your password after first login. You can run the **terminal user password** command to modify your password.

Copyright © Huawei Technologies Co., Ltd.

Follow-up Procedure

- You can run the **idle-timeout** command to set the terminal timeout time. if you do not input commands within the specified timeout time, the system disconnects the terminal. By default, the terminal timeout time is set to 5 minutes. If you do not run any commands within 5 minutes, the system disconnects with the terminal. To perform any operation, you must have to log in to the system again.
- In the commissioning procedure, you must use the command, It is recommended that you know well the command modes first.**Figure 1-17** shows how to switch command modes.

Figure 1-17



1.3.5.3 Login Through Telnet (Inband Management)

This topic describes how to log in to the MA5600T/MA5603T/MA5608T using the upstream port (inband management port) in the telnet mode to maintain and manage the MA5600T/MA5603T/MA5608T. You are advised to use SSH mode.

Prerequisites

Engineers are logged in to the MA5600T/MA5603T/MA5608T by using the local serial port or the ETH port.

NOTE

The default IP address of the maintenance Ethernet port (ETH port on the control board) is 10.11.104.2, and the subnet mask is 255.255.255.0.

- For details about how to log in to the MA5600T/MA5603T/MA5608T by using the local serial port, see **1.3.5.1 Login Through the Local Serial Port**.
- For details about how to log in to the MA5600T/MA5603T/MA5608T by using the ETH port, see the following:
  - Configure the IP address of the PC that is used for logging in to the MA5600T/MA5603T/MA5608T. This IP address is on the same subnet as the IP address of the maintenance Ethernet port but is not the IP address of the maintenance Ethernet port. For example, configure the IP address to 10.11.104.6.
  - After logging in to the MA5600T/MA5603T/MA5608T, run the **ip address** command to change the IP address of the device to 10.50.1.10/24.
  - Change the IP address of the PC to be on the same subnet as the IP address of the maintenance Ethernet port but is not the IP address of the maintenance Ethernet port. For example, change the IP address of the device to 10.50.1.11/24.

Networking

Figure 1-18 shows an example network for inband management through telnet in a LAN, and **Figure 1-19** shows an example network for inband management through telnet in a WAN.

Copyright © Huawei Technologies Co., Ltd.

NOTE

In this network, the SCUB control board (in slot 9 or 10) is used for upstream transmission, and the upstream port is 0/19/0. In addition, the GIU upstream interface board (in slot 19 or 20) can be used for upstream transmission. Alternatively, you need to run the **electro-switch***0 location-1* command to switch the electronic switch to the GIU upstream interface board for upstream transmission. By default, the electronic switch is in the **location-0** state, which indicates that the control board is used for upstream transmission.

Figure 1-18 Example network for inband management through telnet in a LAN

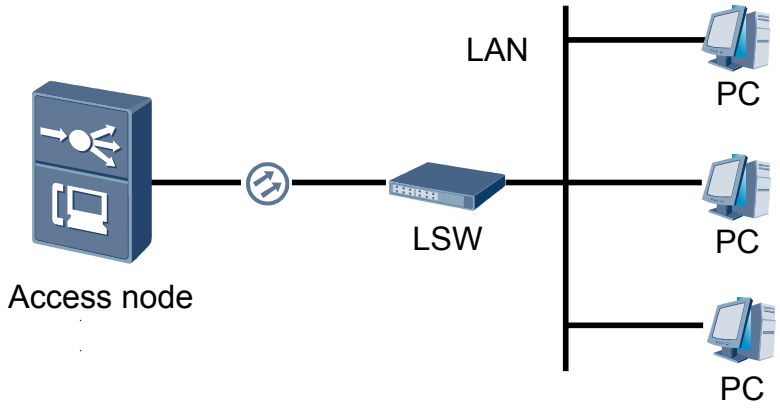
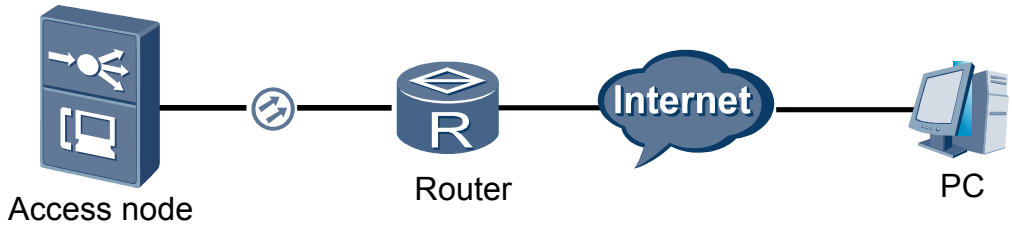


Figure 1-19 Example network for inband management through telnet in a WAN



Data Plan

Table 1-14 and Table 1-15 provide the data plan for the inband management through telnet in a LAN and in a WAN respectively.

Table 1-14 Data plan for the inband management through telnet in a LAN

Item	Data
Upstream port of the MA5600T/MA5603T/ MA5608T	● VLAN ID: 30 ● Port: 0/19/0 ● IP address: 10.50.1.10/24

Copyright © Huawei Technologies Co., Ltd.

Item	Data
Maintenance terminal	IP address: 10.50.1.20/24 (in the same subnet as the IP address of the maintenance Ethernet port)

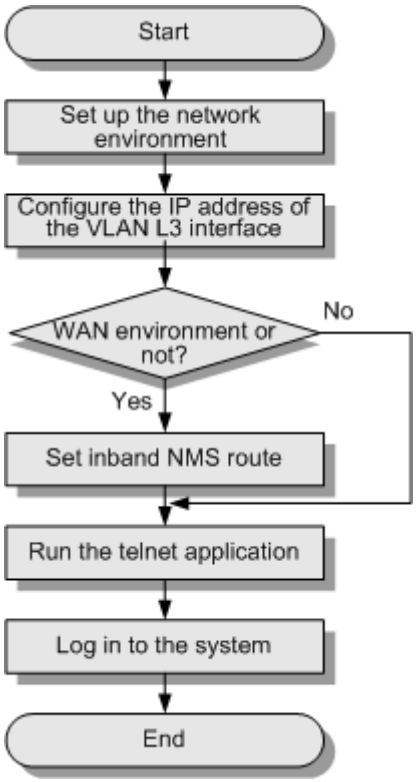
Table 1-15 Data plan for the inband management through telnet in a WAN

Item	Data
Upstream port of the MA5600T/MA5603T/ MA5608T	● VLAN ID: 30 ● Port: 0/19/0 ● IP address: 10.50.1.10/24
Maintenance terminal	IP address: 10.10.1.10/24
Router port connecting to the MA5600T/ MA5603T/MA5608T	IP address: 10.50.1.1/24

Flowchart

Figure 1-20 shows the flowchart for logging in to the MA5600T/MA5603T/MA5608T through telnet (inband management).

Figure 1-20 Flowchart for logging in to the MA5600T/MA5603T/MA5608T through telnet (inband management)



Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Set up the network environment.

- If you log in to the MA5600T/MA5603T/MA5608T in the LAN inband management mode through telnet, set up a network environment according to **Figure 1-18**.
- If you log in to the MA5600T/MA5603T/MA5608T in the WAN inband management mode through telnet, set up a network environment according to **Figure 1-19**.

Step 2 Configure the IP address of the VLAN Layer 3 interface.

1. Run the **vlan** command to create a management VLAN.

   ```
   huawei(config)#vlan 30 standard
   ```

2. Run the **port vlan** command to add an upstream port to the VLAN.

   ```
   huawei(config)#port vlan 30 0/19 0
   ```

3. In the VLANIF mode, run the **ip address** command to configure the IP address of the VLAN Layer 3 interface.

   ```
   huawei(config)#interface vlanif 30
   huawei(config-if-vlanif30)#ip address 10.50.1.10 24
   huawei(config-if-vlanif30)#quit
   ```

NOTE

If the packet transmitted from the upstream port is untagged, run the **native-vlan** command to configure the native VLAN of the upstream port to be the same as the VLAN of the upstream port.

Step 3 Add a route for the inband management.

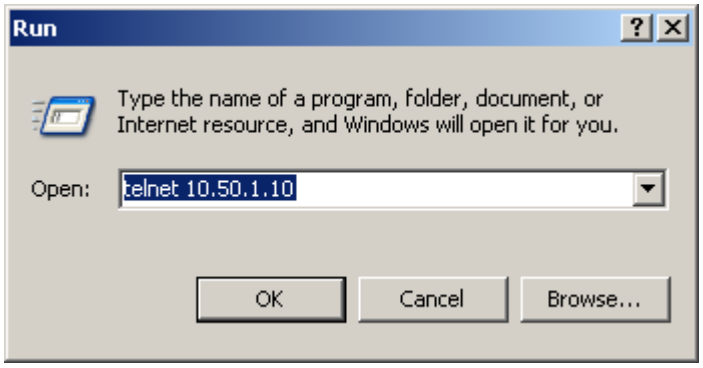
- If the network environment is set up as shown in **Figure 1-18**, you need not add a route.
- If the network environment is set up as shown in **Figure 1-19**, run the **ip route-static** command to add a route from the maintenance Ethernet port of the MA5600T/MA5603T/MA5608T to the maintenance terminal.

  ```
  huawei(config)#ip route-static 10.10.1.0 24 10.50.1.1
  ```

Step 4 Run the telnet application.

On the maintenance terminal, choose **Start** > **Run**. On the **Run** window, input "telnet 10.50.1.10" in the **Open** field as shown in **Figure 1-21** (considering the Windows OS as an example), and click **OK**. Then, the telnet dialog box is displayed.

Figure 1-21 Running the telnet application



Copyright © Huawei Technologies Co., Ltd.

Step 5 Log in to the system.

In the telnet dialog box, input the user name and the password. By default, the user name is **root**, and the password is **admin**. When the login is successful, the system displays the following information:

```
>>User name:root
>>User password:admin

 Huawei Integrated Access SoftwareMA5600T/MA5603T/MA5608T.
  Copyright(C) Huawei Technologies Co., Ltd. 2002-2012. All rights reserved.

  ------------------------------------------------------------------------------
  User last login information:
  ------------------------------------------------------------------------------
  Access Type : Telnet
  IP-Address  : 10.10.10.122
  Login  Time : 2011-03-29 16:03:20+08:00
  Logout Time : 2011-03-29 16:08:40+08:00
  ------------------------------------------------------------------------------
  ------------------------------------------------------------------------------
  User fail login information:
  ------------------------------------------------------------------------------
  Last Access Type    : Telnet
  Last IP-Address     : 10.10.10.74
  Last Login Time     : 2011-03-29 16:11:10+08:00
  Login Failure Times : 2
  ------------------------------------------------------------------------------
  ------------------------------------------------------------------------------
  All user fail login information:
  ------------------------------------------------------------------------------
  Access Type IP-Address           Time                          Login Times
  ------------------------------------------------------------------------------
  Telnet      10.10.10.74          2011-03-29 16:11:10+08:00               1
  Telnet      10.10.10.122         2011-03-29 15:37:05+08:00               3
  Telnet      10.10.10.193         2011-03-25 18:19:04+08:00               1
  ------------------------------------------------------------------------------
```

The following table describes the parameters in response to this login.

Parameter	Description
User name	Indicates the user name.
User password	Indicates the user password that is not displayed on the maintenance terminal.
User last login information	Indicates the information about the latest successful login.
Access Type	Indicates the access type of the latest successful login.
IP-Address	Indicates the IP address of the latest successful login.
Login Time	Indicates the time of the latest successful login.
Logout Time	Indicates the time of the latest successful logout. If the user does not log out, it displays as "--".
User fail login information	Indicates the information about the failed login.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Last Access Type	Indicates the access type of the latest failed login.
Last IP-Address	Indicates the IP address of the latest failed login.
Last Login Time	Indicates the time of the latest failed login.
Login Failure Times	Indicates the failed login times. It is the times of login failures between two login successes, but not the accumulative login failures.
All user fail login information	Indicates the information about failed login of all users, which can be viewed only by user root or security administrator.
Access Type	Indicates the access type of the login.
IP-Address	Indicates the IP address of the login.
Time	Indicates the time of the login.
Login Times	Indicates the login times.

----End

Result

After logging in to the system, you can maintain and manage the MA5600T/MA5603T/MA5608T.

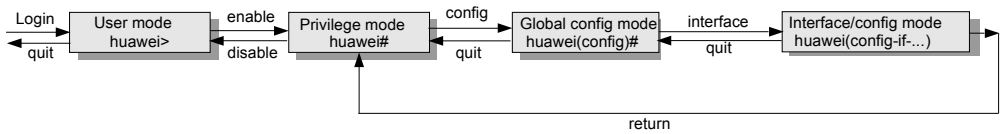
NOTE

To improve the system security, please modify your password after first login. You can run the **terminal user password** command to modify your password.

Follow-up Procedure

- You can run the **idle-timeout** command to set the terminal timeout time. if you do not input commands within the specified timeout time, the system disconnects the terminal. By default, the terminal timeout time is set to 5 minutes. If you do not run any commands within 5 minutes, the system disconnects with the terminal. To perform any operation, you must have to log in to the system again.
- In the commissioning procedure, you must use the command, It is recommended that you know well the command modes first.**Figure 1-22** shows how to switch command modes.

Figure 1-22



Copyright © Huawei Technologies Co., Ltd.

1.3.5.4 Login Through SSH (Outband Management)

This topic describes how to log in to the MA5600T/MA5603T/MA5608T using the local maintenance Ethernet port (outband management port) in the secure shell (SSH) mode to maintain and manage the MA5600T/MA5603T/MA5608T. The SSH provides authentication, encryption, and authorization to ensure the network communication security. When a user logs in to the MA5600T/MA5603T/MA5608T remotely over an insecure network, SSH provides security guarantee and powerful authentication to protect the MA5600T/MA5603T/MA5608T against attacks such as IP address spoofing and interception of plain text password.

Prerequisites

Engineers are logged in to the MA5600T/MA5603T/MA5608T by using the local serial port or the ETH port.

NOTE

The default IP address of the maintenance Ethernet port (ETH port on the control board) is 10.11.104.2, and the subnet mask is 255.255.255.0.

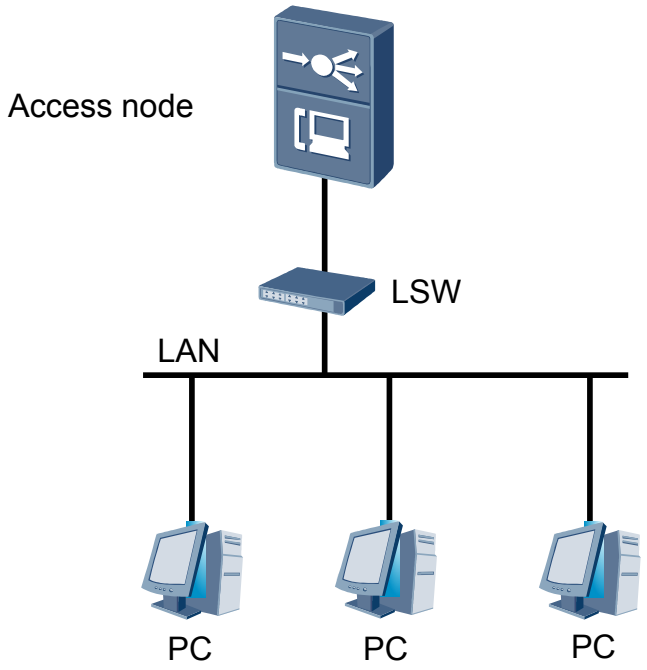
- For details about how to log in to the MA5600T/MA5603T/MA5608T by using the local serial port, see **1.3.5.1 Login Through the Local Serial Port**.
- For details about how to log in to the MA5600T/MA5603T/MA5608T by using the ETH port, see the following:
  - Configure the IP address of the PC that is used for logging in to the MA5600T/MA5603T/MA5608T. This IP address is on the same subnet as the IP address of the maintenance Ethernet port but is not the IP address of the maintenance Ethernet port. For example, configure the IP address to 10.11.104.6.
  - After logging in to the MA5600T/MA5603T/MA5608T, run the **ip address** command to change the IP address of the device to 10.50.1.10/24.
  - Change the IP address of the PC to be on the same subnet as the IP address of the maintenance Ethernet port but is not the IP address of the maintenance Ethernet port. For example, change the IP address of the device to 10.50.1.11/24.

Networking

Figure 1-23 shows an example network for outband management through SSH in a LAN, and **Figure 1-24** shows an example network for outband management through SSH in a WAN.

Copyright © Huawei Technologies Co., Ltd.

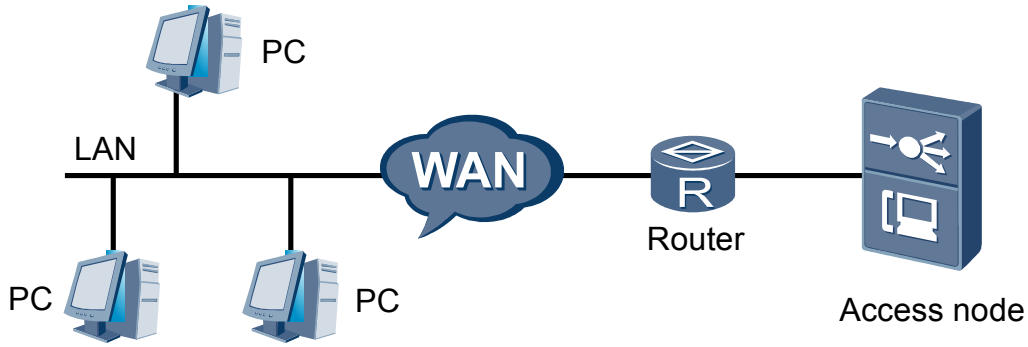
Figure 1-23 Example network for outband management through SSH in a LAN



NOTE

The MA5600T/MA5603T/MA5608T is connected to the LAN using the straight using cable, and the IP address of the maintenance Ethernet port of the MA5600T/MA5603T/MA5608T is in the same network segment as the IP address of the maintenance terminal. Alternatively, the Ethernet port of the maintenance terminal can be directly connected to the maintenance Ethernet port of the MA5600T/MA5603T/MA5608T to manage the MA5600T/MA5603T/MA5608T in the outband management mode. In such a condition, if the MA5600T/MA5603T/MA5608T uses SCUL/SCUB control board, and the peer device does not support the cable autosensing function, a crossover cable must be used.

Figure 1-24 Example network for outband management through SSH in a WAN



Data Plan

Table 1-16 and Table 1-17 provide the data plan for the outband management through SSH in a LAN and in a WAN respectively.

Copyright © Huawei Technologies Co., Ltd.

Table 1-16 Data plan for the outband management through SSH in a LAN

Item	Data
Maintenance Ethernet port of the MA5600T/ MA5603T/MA5608T	● IP address: 10.50.1.10/24 ● User authentication mode: RSA public key authentication ● RSA key name: key **NOTE** By default, the IP address of the maintenance Ethernet port (ETH port on the control board) is 10.11.104.2, and the subnet mask is 255.255.255.0.
New user	● User name/Password: huawei/test01 ● Authority: Operator ● Permitted reenter number: 4
Maintenance terminal	IP address: 10.50.1.20/24 (in the same subnet as the IP address of the maintenance Ethernet port)

Table 1-17 Data plan for the outband management through SSH in a WAN

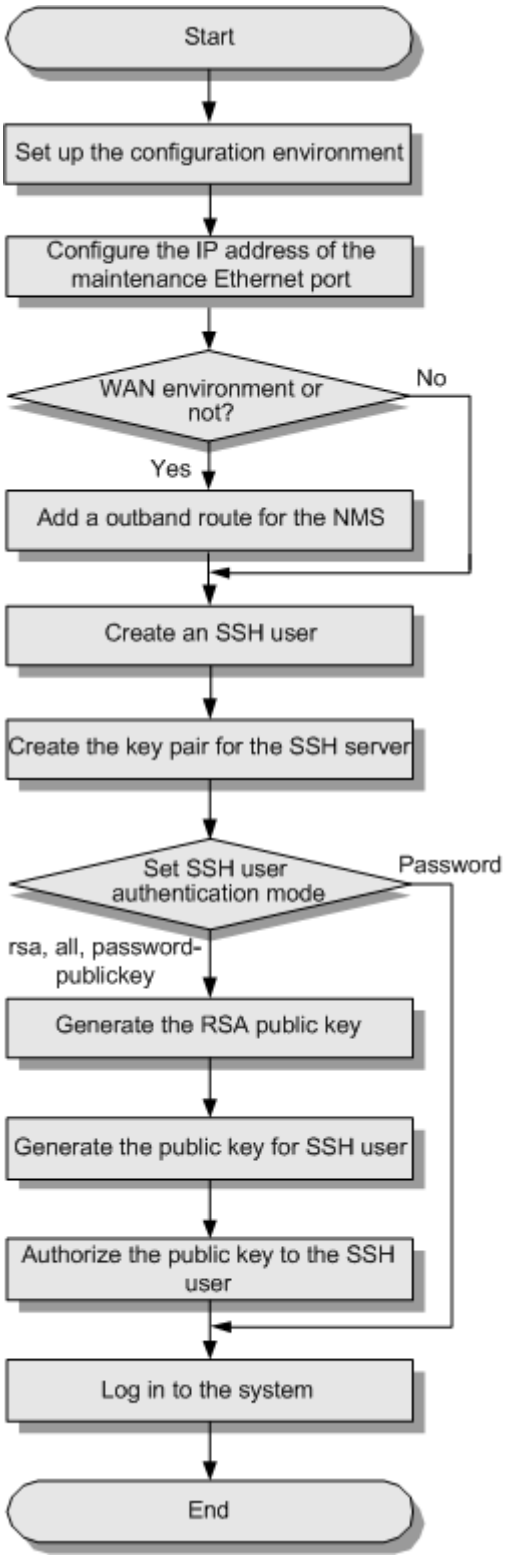
Item	Data
Maintenance Ethernet port of the MA5600T/ MA5603T/MA5608T	● IP address: 10.50.1.10/24 ● User authentication mode: RSA public key authentication ● RSA key name: key **NOTE** By default, the IP address of the maintenance Ethernet port (ETH port on the control board) is 10.11.104.2, and the subnet mask is 255.255.255.0.
New user	● User name/Password: huawei/test01 ● Authority: Operator ● Permitted reenter number: 4
Maintenance terminal	IP address: 10.10.1.10/24
Router port connecting to the MA5600T/ MA5603T/MA5608T	IP address: 10.50.1.1/24

Flowchart

Figure 1-25 shows the flowchart for logging in to the MA5600T/MA5603T/MA5608T through SSH.

Copyright © Huawei Technologies Co., Ltd.

Figure 1-25 Flowchart for logging in to the MA5600T/MA5603T/MA5608T through SSH (Outband Management)



Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Set up the network environment.

- If you log in to the MA5600T/MA5603T/MA5608T in the LAN outband management mode through SSH, set up a network environment according to **Figure 1-23**.
- If you log in to the MA5600T/MA5603T/MA5608T in the WAN outband management mode through SSH, set up a network environment according to **Figure 1-24**.

Step 2 Configure the IP address of the maintenance Ethernet port.

In the MEth mode, run the **ip address** command to configure the IP address of the maintenance Ethernet port.

```
huawei(config)#interface meth 0
huawei(config-if-meth0)#ip address 10.50.1.10 24
huawei(config-if-meth0)#quit
```

Step 3 Add a route for the outband management.

- If the network environment is set up as shown in **Figure 1-23**, you need not add a route.
- If the network environment is set up as shown in **Figure 1-24**, run the **ip route-static** command to add a route from the maintenance Ethernet port of the MA5600T/MA5603T/MA5608T to the maintenance terminal.
  ```
  huawei(config)#ip route-static 10.10.1.0 24 10.50.1.1
  ```

Step 4 Create a user.

Run the **terminal user name** command to create a user.

```
huawei(config)#terminal user name
  User Name(length<6,15>):huawei
  User Password(length<6,15>):test01 //The password is not displayed on the
maintenance terminal.
  Confirm Password(length<6,15>):test01 //The password is not displayed on the
maintenance terminal.
  User profile name(<=15 chars)[root]:
  User's Level:
     1. Common User  2. Operator:2
  Permitted Reenter Number(0--4):4
  User's Appended Info(<=30 chars):
  Adding user succeeds
  Repeat this operation? (y/n)[n]:n
```

Step 5 Create the local RSA key pair.

Run the **rsa local-key-pair create** command to create the local RSA key pair.

NOTICE

The prerequisite for the login through SSH is that the local RSA key pair must be configured and generated. Therefore, before performing other SSH configurations, make sure that the local RSA key pair is generated.

```
huawei(config)#rsa local-key-pair create
The key name will be: Host
The range of public key size is (512 ~ 2048).
NOTES: If the key modulus is greater than 512,
       It will take a few minutes.
Input the bits in the modulus[default = 512]:
Generating keys...
```


Copyright © Huawei Technologies Co., Ltd.

```
..++++++++++++
.....................++++++++++++
.................................++++++++
...........++++++++
```

Step 6 Set the SSH user authentication mode.

Run the **ssh user huawei authentication-type rsa** command to choose the authentication mode of the SSH user.

There are four authentication modes for SSH users, as shown in the following. In this topic, authentication mode **rsa** is considered as an example.

- password: authentication based on a password.
- rsa: authentication based on an RSA public key.
- all: authentication based on a password or an RSA public key. The user can log in to the device either by the password or the RSA public key.
- password-publickey: authentication based on a password and a public key. The user can log in to the device only after both the password and the RSA public key authentication.

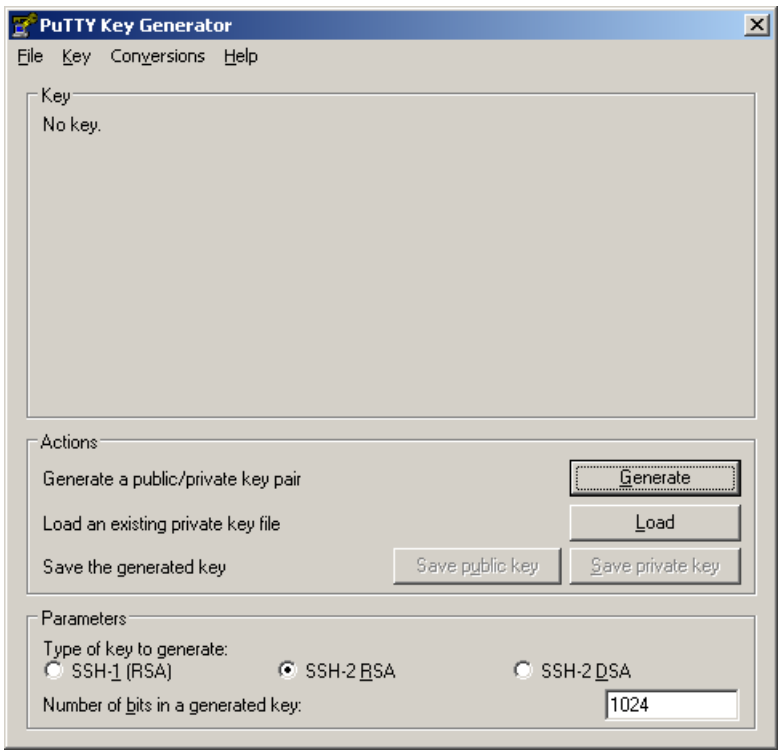
```
huawei(config)#ssh user huawei authentication-type
{ all<K>|password-publickey<K>|password<K>|rsa<K> }:rsa

  Command:
          ssh user huawei authentication-type rsa
%Authentication type setted, and will be in effect next time.
```

Step 7 Generate the RSA public key.

1. Run the key generator.

   Run the client software key generator Puttygen.exe. **Figure 1-26** shows the interface of the key generator.

   Figure 1-26 Interface of the key generator

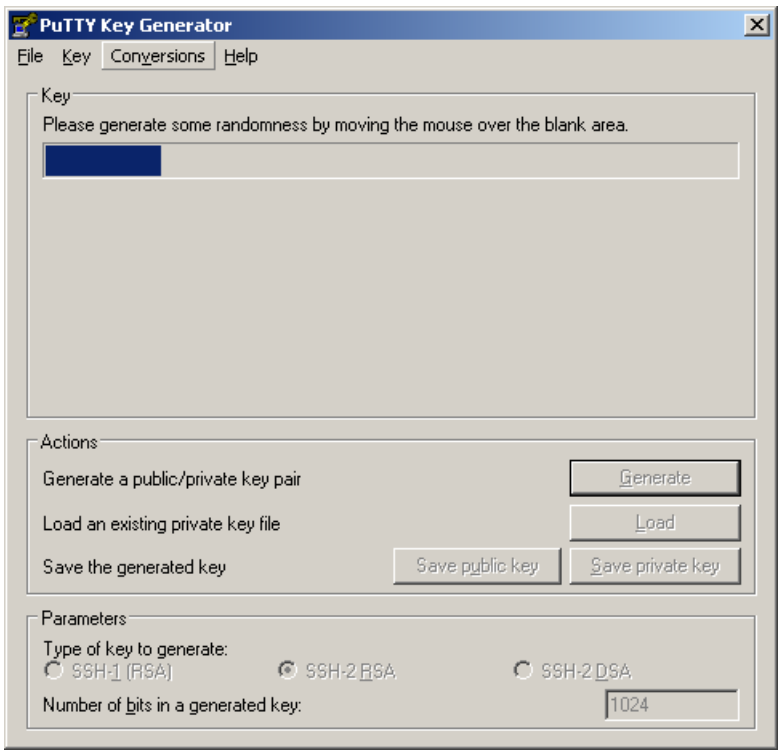


Copyright © Huawei Technologies Co., Ltd.

2. Generate the client key.

   Select **SSH-2 RSA** as the key type under **Parameters**, click **Generate**, and move the cursor according to the prompt on the interface to generate the client key, as shown in **Figure 1-27**.

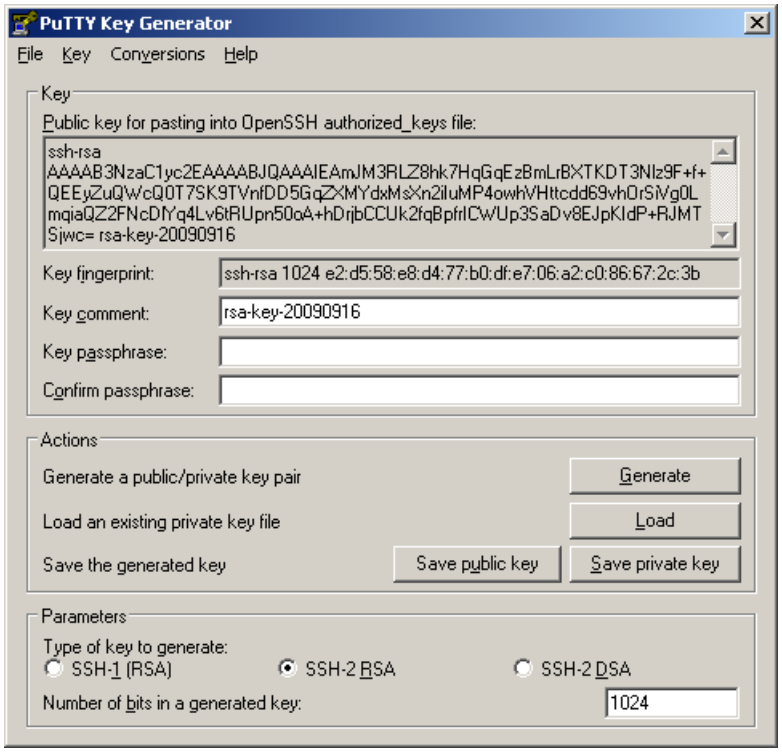
Figure 1-27 Interface of the key generator



Click **Save public key** and **Save private key** to save the public key and the private key respectively after they are generated, as shown in **Figure 1-28**.

Copyright © Huawei Technologies Co., Ltd.

Figure 1-28 Save the public key and the private key

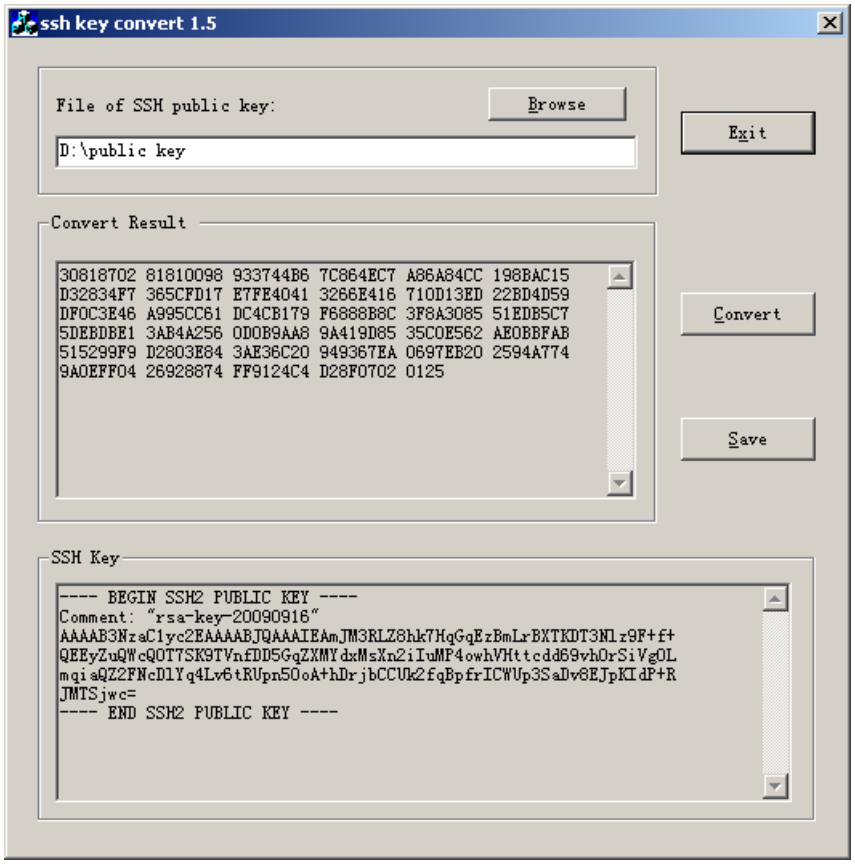


3. Generate the RSA public key.

   Open sshkey.exe, click **Browse**, and choose the **public key** file saved in the preceding step. Then, click **Convert** to change the client public key to the RSA public key, as shown in **Figure 1-29**.

Copyright © Huawei Technologies Co., Ltd.

Figure 1-29 Interface of converting the client public key to the RSA public key



Step 8 Generate the public key for the SSH user.

Create RSA public key. Copy the RSA public key to the server in the config-rsa-key-code command line mode.

```
huawei(config)#rsa peer-public-key key
Enter "RSA public key" view, return system view with "peer-public-key end".
NOTE: The number of the bits of public key must be between 769 and 2048.

huawei(config-rsa-public-key)#public-key-code begin
Enter "RSA key code" view, return last view with "public-key-code end".

huawei(config-rsa-key-code)#30818702 81810098 933744B6 7C864EC7 A86A84CC 198BAC1
5

huawei(config-rsa-key-code)#D32834F7 365CFD17 E7FE4041 3266E416 710D13ED 22BD4D5
9

huawei(config-rsa-key-code)#DF0C3E46 A995CC61 DC4CB179 F6888B8C 3F8A3085 51EDB5C
7

huawei(config-rsa-key-code)#5DEBDBE1 3AB4A256 0D0B9AA8 9A419D85 35C0E562 AE0BBFA
B

huawei(config-rsa-key-code)#515299F9 D2803E84 3AE36C20 949367EA 0697EB20 2594A77
4

huawei(config-rsa-key-code)#9A0EFF04 26928874 FF9124C4 D28F0702 0125
```


Copyright © Huawei Technologies Co., Ltd.

```
huawei(config-rsa-key-code)#public-key-code end

huawei(config-rsa-public-key)#peer-public-key end
```

Step 9 Assign the public key to the SSH user.

Run the **ssh user assign rsa-key** command to assign the RSA public key to the SSH user.

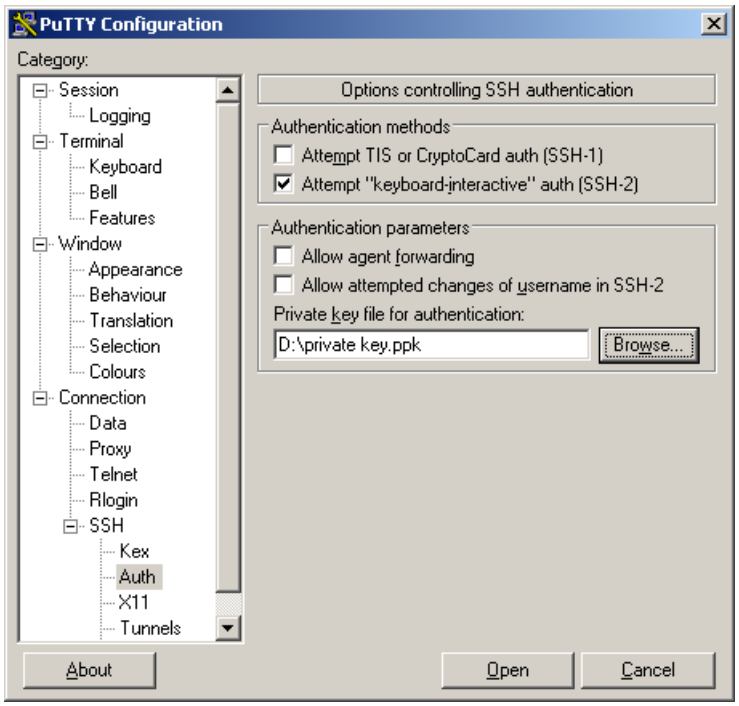
```
huawei(config)#ssh user huawei assign rsa-key key
```

Step 10 Log in to the system.

1. Run the client software.

   Run the SSH client software putty.exe, choose **SSH** > **Auth** from the navigation tree, and assign a file for the RSA private key, as shown in **Figure 1-30**. Click **Browse** to display the window for selecting the file. In the window, select the file for the private key, and click **OK**.

   Figure 1-30 Interface of the SSH client software

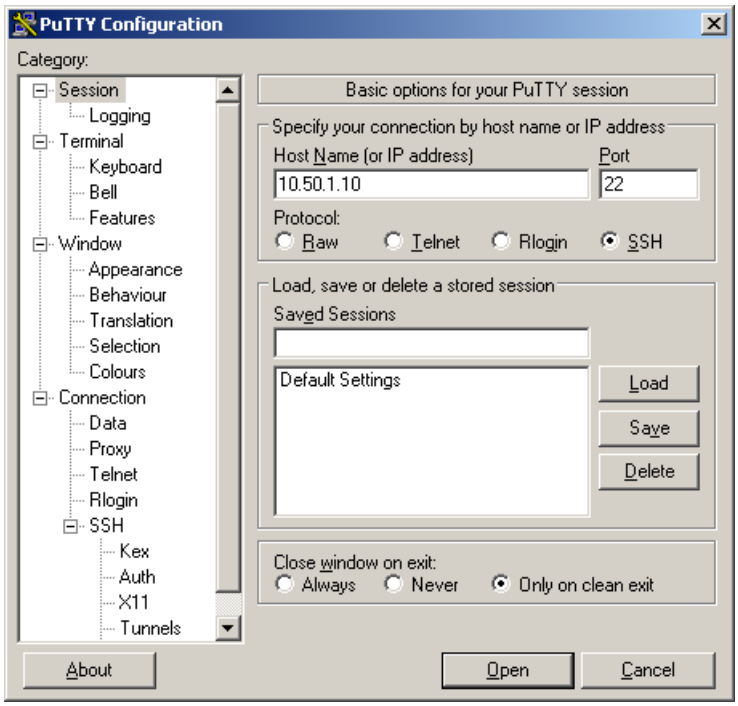


2. Log in to the system.

   Choose **Session** from the navigation tree, and then input the IP address of the MA5600T/MA5603T/MA5608T in the **Host Name (or IP address)** field, as shown in **Figure 1-31**. Then, click **Open** to log in to the system.

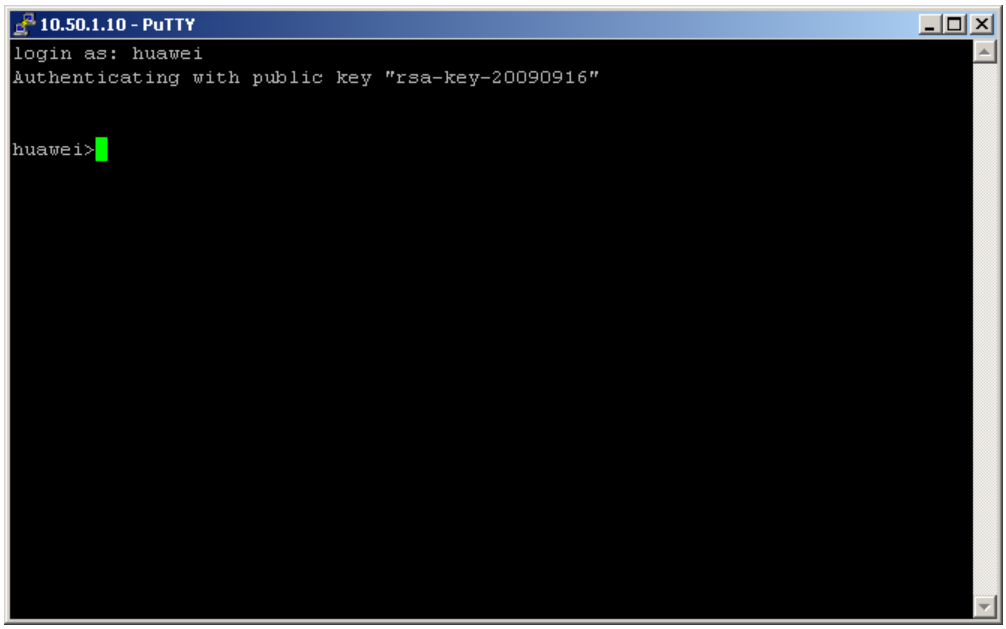
Copyright © Huawei Technologies Co., Ltd.

Figure 1-31 Interface for logging in to the system using the SSH client software



The user authentication mode is set to the RSA authentication mode, and the system therefore displays the prompt, as shown in **Figure 1-32**. Input the user name to log in to the system (here, the user name is **huawei**).

Figure 1-32 Interface for logging in to the system using the SSH client software



----End

Copyright © Huawei Technologies Co., Ltd.

Result

After logging in to the system, you can maintain and manage the MA5600T/MA5603T/MA5608T.

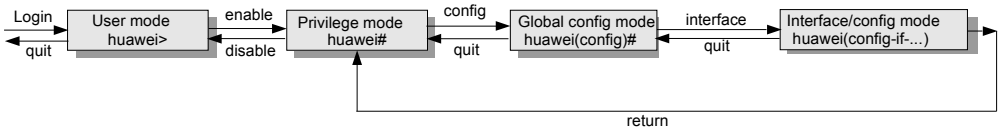
NOTE

To improve the system security, please modify your password after first login. You can run the **terminal user password** command to modify your password.

Follow-up Procedure

- You can run the **idle-timeout** command to set the terminal timeout time. if you do not input commands within the specified timeout time, the system disconnects the terminal. By default, the terminal timeout time is set to 5 minutes. If you do not run any commands within 5 minutes, the system disconnects with the terminal. To perform any operation, you must have to log in to the system again.
- In the commissioning procedure, you must use the command, It is recommended that you know well the command modes first.**Figure 1-33** shows how to switch command modes.

Figure 1-33



1.3.5.5 Login Through SSH (Inband Management)

This topic describes how to log in to the MA5600T/MA5603T/MA5608T using the upstream port (inband management port) in the secure shell (SSH) mode to maintain and manage the MA5600T/MA5603T/MA5608T. The SSH provides authentication, encryption, and authorization to ensure the network communication security. When a user logs in to the MA5600T/MA5603T/MA5608T remotely over an insecure network, SSH provides security guarantee and powerful authentication to protect the MA5600T/MA5603T/MA5608T against attacks such as IP address spoofing and interception of plain text password.

Prerequisites

Engineers are logged in to the MA5600T/MA5603T/MA5608T by using the local serial port or the ETH port.

NOTE

The default IP address of the maintenance Ethernet port (ETH port on the control board) is 10.11.104.2, and the subnet mask is 255.255.255.0.

- For details about how to log in to the MA5600T/MA5603T/MA5608T by using the local serial port, see **1.3.5.1 Login Through the Local Serial Port**.
- For details about how to log in to the MA5600T/MA5603T/MA5608T by using the ETH port, see the following:
  - Configure the IP address of the PC that is used for logging in to the MA5600T/MA5603T/MA5608T. This IP address is on the same subnet as the IP address of the

Copyright © Huawei Technologies Co., Ltd.

maintenance Ethernet port but is not the IP address of the maintenance Ethernet port. For example, configure the IP address to 10.11.104.6.

- After logging in to the MA5600T/MA5603T/MA5608T, run the **ip address** command to change the IP address of the device to 10.50.1.10/24.
- Change the IP address of the PC to be on the same subnet as the IP address of the maintenance Ethernet port but is not the IP address of the maintenance Ethernet port. For example, change the IP address of the device to 10.50.1.11/24.

Networking

Figure 1-34 shows an example network for inband management through SSH in a LAN, and **Figure 1-35** shows an example network for inband management through SSH in a WAN.

NOTE

In this network, the SCUB control board (in slot 9 or 10) is used for upstream transmission, and the upstream port is 0/9/0. Alternatively, the GIU upstream interface board (in slot 19 or 20) can be used for upstream transmission. In this case, you need to run the **electro-switch***0 location-1* command to switch the electronic switch to the GIU upstream interface board for upstream transmission. By default, the electronic switch is in the **location-0** state, which indicates the control board is used for upstream transmission.

Figure 1-34 Example network for inband management through SSH in a LAN

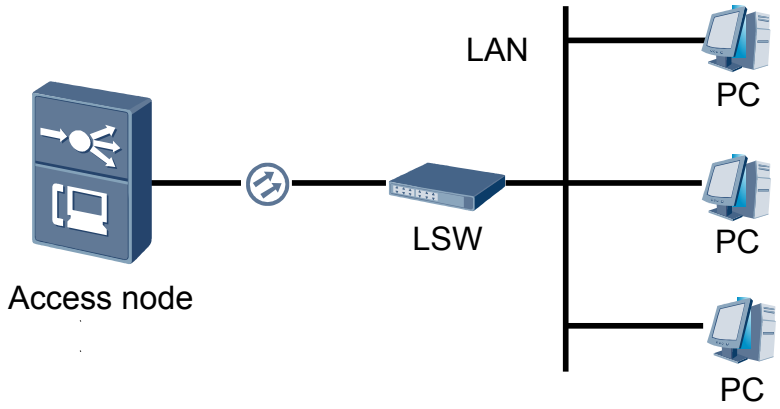
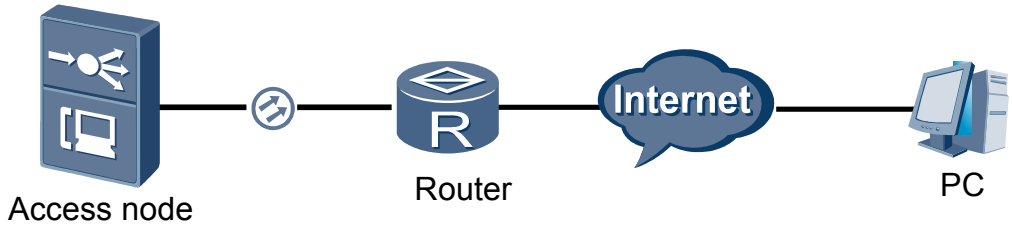


Figure 1-35 Example network for inband management through SSH in a WAN



Copyright © Huawei Technologies Co., Ltd.

Data Plan

Table 1-18 and Table 1-19 provide the data plan for the inband management through SSH in a LAN and in a WAN respectively.

Table 1-18 Data plan for the inband management through SSH in a LAN

Item	Data
Upstream port of the MA5600T/MA5603T/MA5608T	● VLAN ID: 30 ● Port: 0/9/0 ● IP address: 10.50.1.10/24 ● User authentication mode: RSA public key authentication ● RSA key name: key
New user	● User name/Password: huawei/test01 ● Authority: Operator ● Permitted reenter number: 4
Maintenance terminal	IP address: 10.50.1.20/24 (in the same subnet as the IP address of the maintenance Ethernet port)

Table 1-19 Data plan for the inband management through SSH in a WAN

Item	Data
Upstream port of the MA5600T/MA5603T/MA5608T	● VLAN ID: 30 ● Port: 0/9/0 ● IP address: 10.50.1.10/24 ● User authentication mode: RSA public key authentication ● RSA key name: key
New user	● User name/Password: huawei/test01 ● Authority: Operator ● Permitted reenter number: 4
Maintenance terminal	IP address: 10.10.1.10/24
Router port connecting to the MA5600T/MA5603T/MA5608T	IP address: 10.50.1.1/24

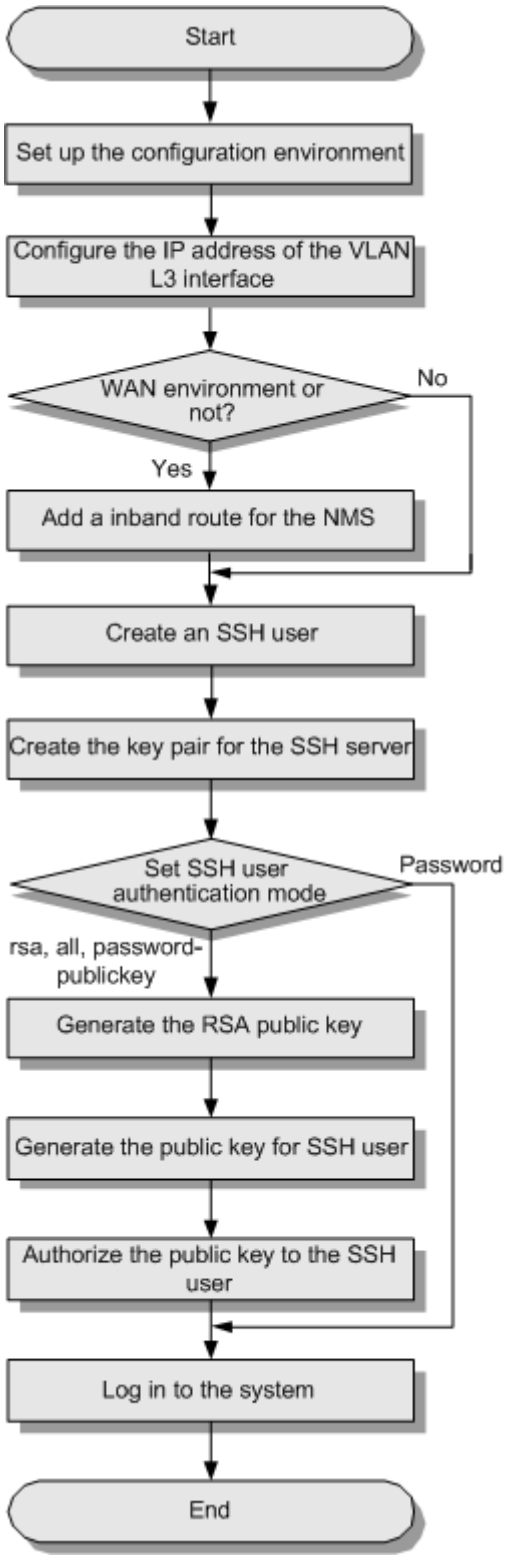
Copyright © Huawei Technologies Co., Ltd.

Flowchart

Figure 1-36 shows the flowchart for logging in to the MA5600T/MA5603T/MA5608T through SSH.

Copyright © Huawei Technologies Co., Ltd.

Figure 1-36 Flowchart for logging in to the MA5600T/MA5603T/MA5608T through SSH (Inband Management)



Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Set up the network environment.

- If you log in to the MA5600T/MA5603T/MA5608T in the LAN inband management mode through SSH, set up a network environment according to **Figure 1-34**.
- If you log in to the MA5600T/MA5603T/MA5608T in the WAN inband management mode through SSH, set up a network environment according to **Figure 1-35**.

Step 2 Configure the IP address of the VLAN Layer 3 interface.

1. Run the **vlan** command to create a management VLAN.

   huawei(config)#**vlan 30 standard**

2. Run the **port vlan** command to add an upstream port to the VLAN.

   huawei(config)#**port vlan 30 0/9 0**

3. In the VLANIF mode, run the **ip address** command to configure the IP address of the VLAN Layer 3 interface.

```
huawei(config)#interface vlanif 30
huawei(config-if-vlanif30)#ip address 10.50.1.10 24
huawei(config-if-vlanif30)#quit
```

NOTE

If the packet transmitted from the upstream port is untagged, run the **native-vlan** command to configure the native VLAN of the upstream port to be the same as the VLAN of the upstream port.

Step 3 Add a route for the inband management.

- If the network environment is set up as shown in **Figure 1-34**, you need not add a route.
- If the network environment is set up as shown in **Figure 1-35**, run the **ip route-static** command to add a route from the maintenance Ethernet port of the MA5600T/MA5603T/MA5608T to the maintenance terminal.

```
huawei(config)#ip route-static 10.10.1.0 24 10.50.1.1
```

Step 4 Create a user.

Run the **terminal user name** command to create a user.

```
huawei(config)#terminal user name
  User Name(length<6,15>):huawei
  User Password(length<6,15>):test01 //The password is not displayed on the
maintenance terminal.
  Confirm Password(length<6,15>):test01 //The password is not displayed on the
maintenance terminal.
  User profile name(<=15 chars)[root]:
  User's Level:
     1. Common User  2. Operator:2
  Permitted Reenter Number(0--4):4
  User's Appended Info(<=30 chars):
  Adding user succeeds
  Repeat this operation? (y/n)[n]:n
```

Step 5 Create the local RSA key pair.

Run the **rsa local-key-pair create** command to create the local RSA key pair.

Copyright © Huawei Technologies Co., Ltd.

NOTICE

The prerequisite for the login through SSH is that the local RSA key pair must be configured and generated. Therefore, before performing other SSH configurations, make sure that the local RSA key pair is generated.

```
huawei(config)#rsa local-key-pair create
The key name will be: Host
The range of public key size is (512 ~ 2048).
NOTES: If the key modulus is greater than 512,
       It will take a few minutes.
Input the bits in the modulus[default = 512]:
Generating keys...
..++++++++++++
.....................++++++++++++
.................................++++++++
...........++++++++
```

Step 6 Set the SSH user authentication mode.

Run the **ssh user huawei authentication-type rsa** command to choose the authentication mode of the SSH user.

There are four authentication modes for SSH users, as shown in the following. In this topic, authentication mode **rsa** is considered as an example.

- password: authentication based on a password.
- rsa: authentication based on an RSA public key.
- all: authentication based on a password or an RSA public key. The user can log in to the device either by the password or the RSA public key.
- password-publickey: authentication based on a password and a public key. The user can log in to the device only after both the password and the RSA public key authentication.

```
huawei(config)#ssh user huawei authentication-type
{ all<K>|password-publickey<K>|password<K>|rsa<K> }:rsa

  Command:
          ssh user huawei authentication-type rsa
%Authentication type setted, and will be in effect next time.
```

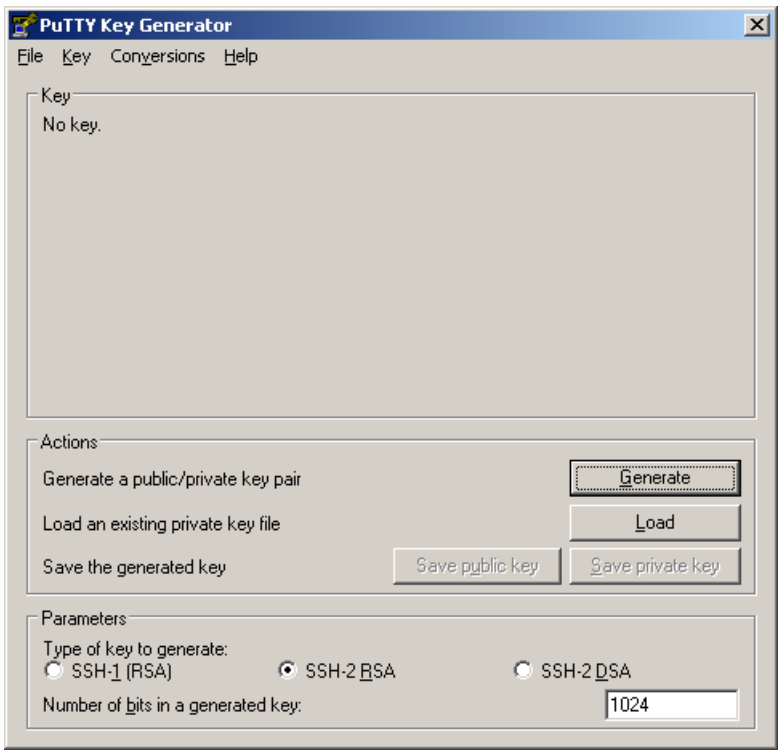
Step 7 Generate the RSA public key.

1. Run the key generator.

   Run the client software key generator Puttygen.exe. **Figure 1-37** shows the interface of the key generator.

Copyright © Huawei Technologies Co., Ltd.

Figure 1-37 Interface of the key generator

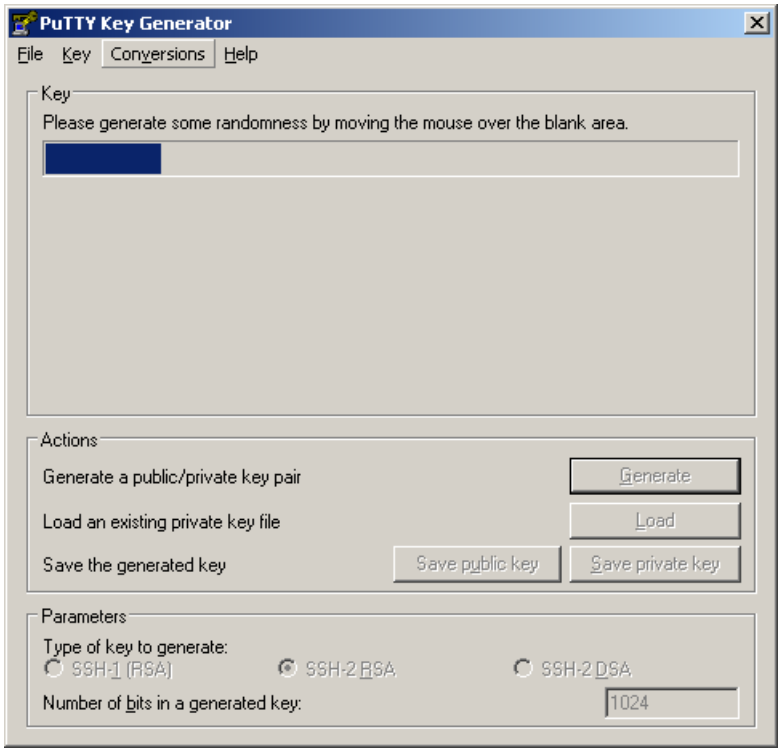


2. Generate the client key.

   Select **SSH-2 RSA** as the key type under **Parameters**, click **Generate**, and move the cursor according to the prompt on the interface to generate the client key, as shown in **Figure 1-38**.

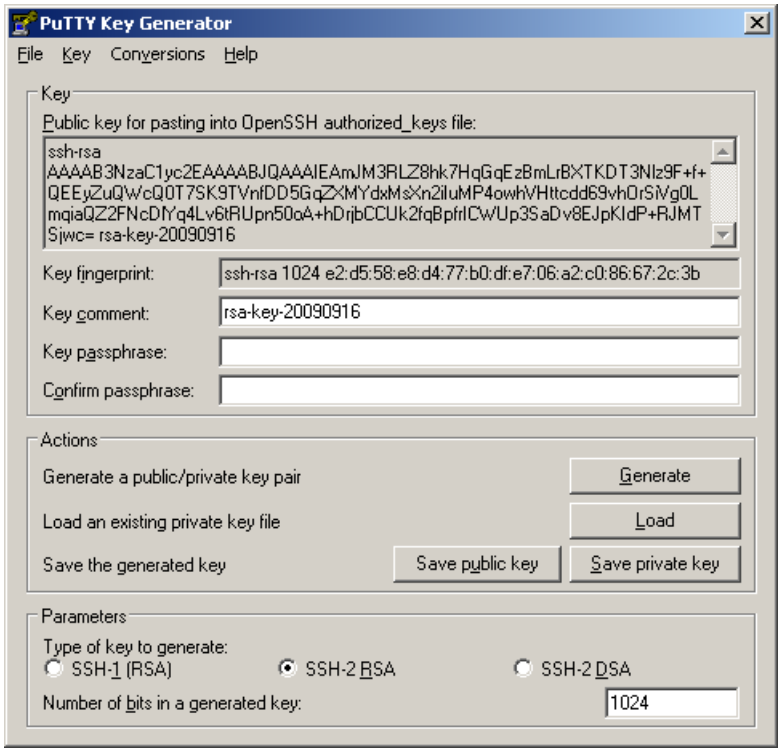
Copyright © Huawei Technologies Co., Ltd.

Figure 1-38 Interface of the key generator



Click **Save public key** and **Save private key** to save the public key and the private key respectively after they are generated, as shown in **Figure 1-39**.

Figure 1-39 Save the public key and the private key

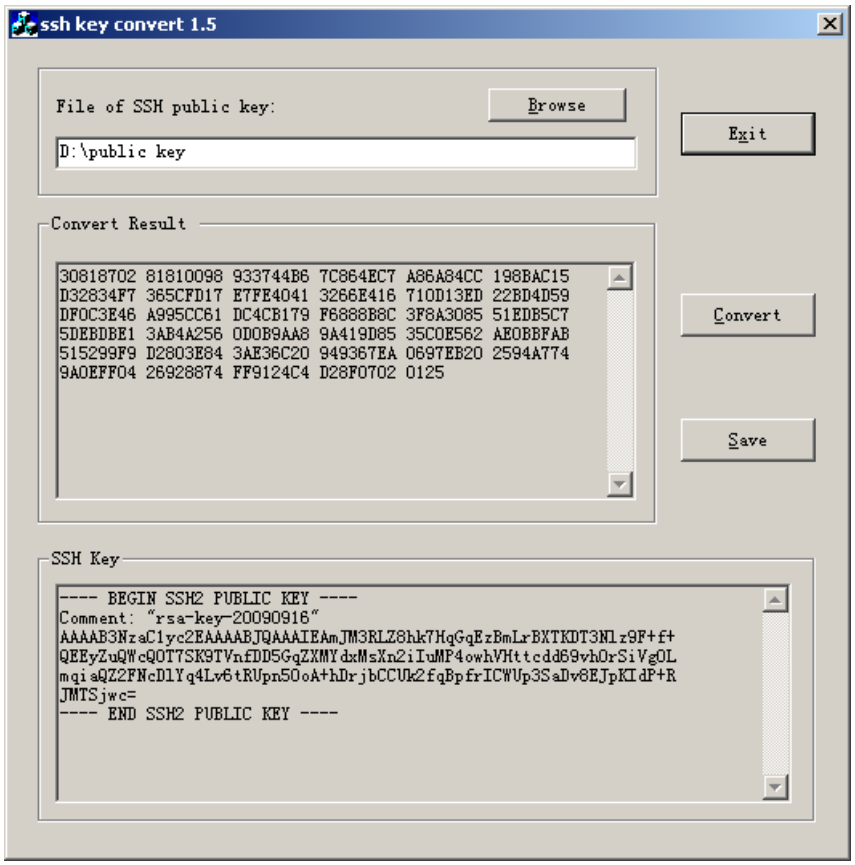


Copyright © Huawei Technologies Co., Ltd.

3. Generate the RSA public key.

   Open sshkey.exe, click **Browse**, and choose the **public key** file saved in the preceding step. Then, click **Convert** to change the client public key to the RSA public key, as shown in **Figure 1-40**.

   Figure 1-40 Interface of converting the client public key to the RSA public key



Step 8 Generate the public key for the SSH user.

Create RSA public key. Copy the RSA public key to the server in the config-rsa-key-code command line mode.

```
huawei(config)#rsa peer-public-key key
Enter "RSA public key" view, return system view with "peer-public-key end".
NOTE: The number of the bits of public key must be between 769 and 2048.

huawei(config-rsa-public-key)#public-key-code begin
Enter "RSA key code" view, return last view with "public-key-code end".

huawei(config-rsa-key-code)#30818702 81810098 933744B6 7C864EC7 A86A84CC 198BAC1
5

huawei(config-rsa-key-code)#D32834F7 365CFD17 E7FE4041 3266E416 710D13ED 22BD4D5
9

huawei(config-rsa-key-code)#DF0C3E46 A995CC61 DC4CB179 F6888B8C 3F8A3085 51EDB5C
7
```


Copyright © Huawei Technologies Co., Ltd.

```
huawei(config-rsa-key-code)#5DEBDBE1 3AB4A256 0D0B9AA8 9A419D85 35C0E562 AE0BBFA
B

huawei(config-rsa-key-code)#515299F9 D2803E84 3AE36C20 949367EA 0697EB20 2594A77
4

huawei(config-rsa-key-code)#9A0EFF04 26928874 FF9124C4 D28F0702 0125

huawei(config-rsa-key-code)#public-key-code end

huawei(config-rsa-public-key)#peer-public-key end
```

Step 9 Assign the public key to the SSH user.

Run the **ssh user assign rsa-key** command to assign the RSA public key to the SSH user.

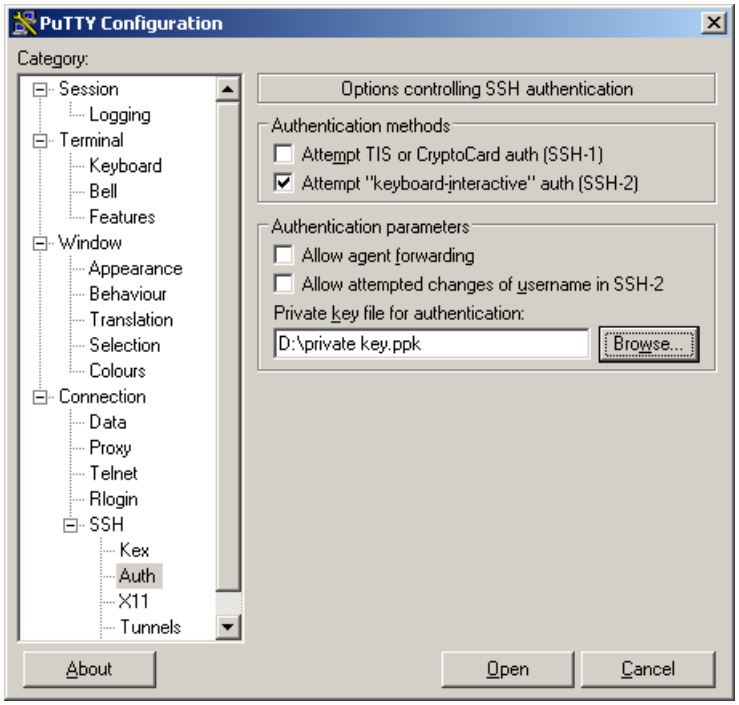
```
huawei(config)#ssh user huawei assign rsa-key key
```

Step 10 Log in to the system.

1. Run the client software.

   Run the SSH client software putty.exe, choose **SSH** > **Auth** from the navigation tree, and assign a file for the RSA private key, as shown in **Figure 1-41**. Click **Browse** to display the window for selecting the file. In the window, select the file for the private key, and click **OK**.

   Figure 1-41 Interface of the SSH client software

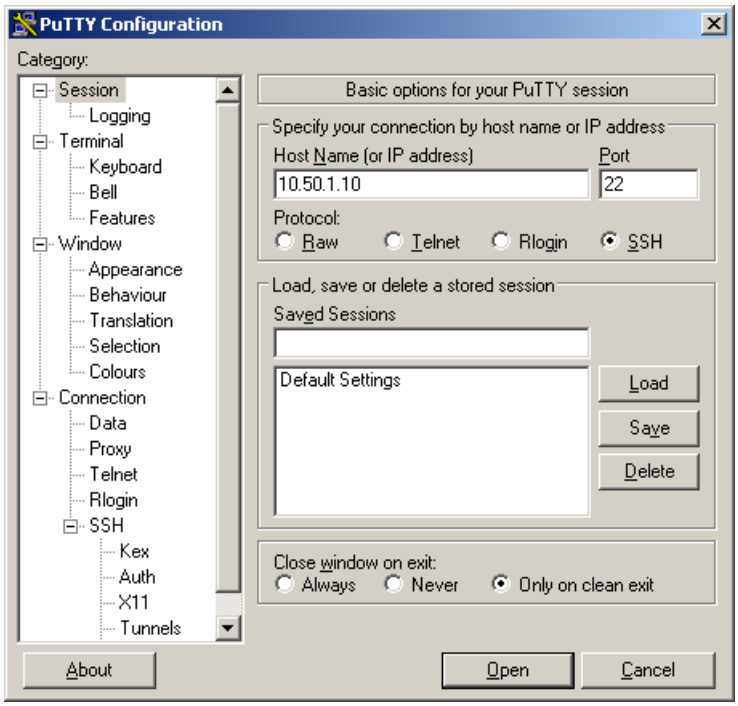


2. Log in to the system.

   Choose **Session** from the navigation tree, and then input the IP address of the MA5600T/MA5603T/MA5608T in the **Host Name (or IP address)** field, as shown in **Figure 1-42**. Then, click **Open** to log in to the system.

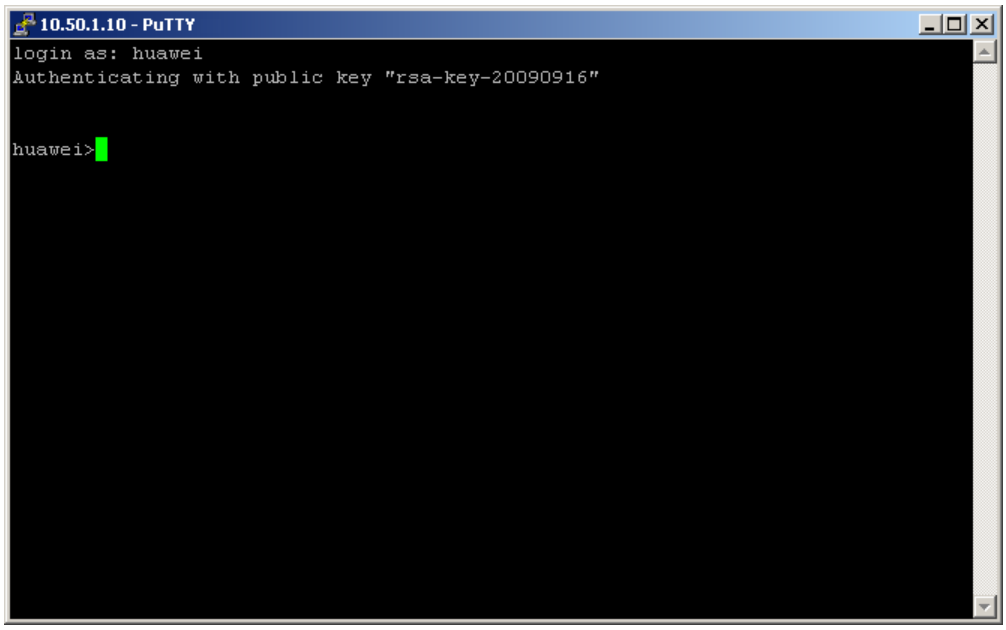
Copyright © Huawei Technologies Co., Ltd.

Figure 1-42 Interface for logging in to the system using the SSH client software



The user authentication mode is set to the RSA authentication mode, and the system therefore displays the prompt, as shown in **Figure 1-43**. Input the user name to log in to the system (here, the user name is **huawei**).

Figure 1-43 Interface for logging in to the system using the SSH client software



----End

Copyright © Huawei Technologies Co., Ltd.

Result

After logging in to the system, you can maintain and manage the MA5600T/MA5603T/MA5608T.

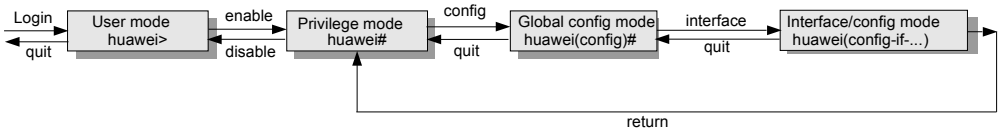
NOTE

To improve the system security, please modify your password after first login. You can run the **terminal user password** command to modify your password.

Follow-up Procedure

- You can run the **idle-timeout** command to set the terminal timeout time. if you do not input commands within the specified timeout time, the system disconnects the terminal. By default, the terminal timeout time is set to 5 minutes. If you do not run any commands within 5 minutes, the system disconnects with the terminal. To perform any operation, you must have to log in to the system again.
- In the commissioning procedure, you must use the command, It is recommended that you know well the command modes first.**Figure 1-44** shows how to switch command modes.

Figure 1-44



1.3.6 Checking the Software State

This topic describes how to verify that current software state meets the deployment requirement.

Procedure

Step 1 Run the **display language** command to check whether the version of the host software meets the deployment requirement.

Step 2 Run the **display patch** command to check whether the version of the patch meets the deployment requirement.

Step 3 Run the **display version** command to check whether the version of the board software meets the deployment requirement.

Step 4 Run the **display board** command to check whether the state of the boards meets the deployment requirement.

- In the integrated access scenario (involving optical, xDSL, and voice access), use the default configurations.
- In the broadband access scenario (involving only optical and xDSL access), use the **system workscene** command to switch the scenario mode of the SCUN board to the **OLT** mode, ensuring that the memory is allocated properly and services are processed smoothly.

----End

Copyright © Huawei Technologies Co., Ltd.

Result

- The version of the host software, the version of the patch, the version of the boards and the state of the board software meet the deployment requirement.
- If the version of the host software and the version of the board software do not meet the deployment requirement, contact the Huawei Customer Service Center. Upgrade the host software if necessary.

Example

To query the host software state that is running in the system, do as follows:

```
huawei>display language
Local:
      Description: CHINESE SIMPLIFIED (DEFAULT LANGUAGE)
      Version:     MA5600V800R0012C00
      Encoding:    GBK

  General:
      Description: ENGLISH (DEFAULT LANGUAGE)
      Version:     MA5600V800R012C00
      Encoding:    ANSIhuawei(config)#display patch
all
  Software Version:MA5600V800R012C00
  ------------------------------------------------------------------------
  Current Patch State:
  ------------------------------------------------------------------------
  Patch Name        Patch State     Delivery     Attribute     Dependency
  ------------------------------------------------------------------------
  ------------------------------------------------------------------------
  Total:0
  Patches in the system cannot be rolled back
huawei>display version
{ <cr>|backplane<K>|frameid/slotid<S><Length 1-15> }:

  Command:
          display version

  VERSION : MA5600V800R012C00
  PRODUCT :

  Active Mainboard Running Area Information:
  -------------------------------------------------
  Current Program Area : Area A
  Current Data Area : Area A

  Program Area A Version : MA5600V800R012C00
  Program Area B Version : MA5600V800R012C00

  Data Area A Version : MA5600V800R012C00
  Data Area B Version : MA5600V800R012C00
  -------------------------------------------------

  Uptime is 0 day(s), 0 hour(s), 0 minute(s), 50 second(s)
huawei#display version
  Main Board: H801SCUN
  ---------------------------------------
  PCB           Version: H801SCUN  VER B
  Base     BIOS Version: 216
  Extended BIOS Version: 222
  Software      Version: MA5600V800R012C00
  Logic         Version: (U48)115
  MAB           Version: 0002

huawei#display board 0
```


Copyright © Huawei Technologies Co., Ltd.

```
  ------------------------------------------------------------------------
  SlotID  BoardName  Status         SubType0 SubType1    Online/Offline
  ------------------------------------------------------------------------
  0
  1       H802ADPD   Normal
  2       H805ADPD   Normal
  3       H801EPBA   Normal
  4
  5
  6
  7       H801GPBC   Normal
  8       H802SHLB   Normal
  9       H801SCUN   Active_normal
  10
  11      H802EDTB   Normal
  12
---- More ( Press 'Q' to break ) ----
```

1.3.7 Loading a Configuration Script

You can run the commands in the configuration script in batches by loading the configuration script instead of running the commands one by one. This shortens the commissioning duration and improves the commissioning efficiency. If you do not use the configuration script to perform the commissioning, skip this operation, and follow the commissioning procedure to perform the subsequent operations.

Prerequisites

- The hardware must be installed and checked.
- The configuration script must be prepared. For details about how to prepare a configuration script, see **1.6.1 Script Making**.
- The TFTP/FTP/SFTP server can normally communicate with the device, and the file path on the server is set correctly before you load the configuration script. For the detailed operation procedure, see **1.6.2 Configuring the File Transfer Mode** .
- The operator is in the privilege mode.

Procedure

- There are two methods for loading the configuration script. You can select one of them.
  - Importing the configuration script
    1. Run the **load configuration** command to load the configuration script on the file server (TFTP/FTP/SFTP server) to the control board of the device.
    2. Run the **active configuration system** command to activate the configuration.
    3. Log in to the system using the user name **root** and password **admin** after the system restarts.
    4. Run the **save** command to save the configuration file and make the new configuration take effect.
  - Copying commands in the configuration script
    1. Open the configuration script, and copy the commands in the configuration script to the command line interface (CLI). However, the following contents must be deleted. Otherwise, the script loading will fail.
       - Delete the following tags.

Copyright © Huawei Technologies Co., Ltd.

```
#
[global-config]
  <global-config>
```

- Delete all the commands related to **terminal user name**.

NOTICE

If you use this method to load the configuration script, you must enter the global config mode. The user level must be operation level at least. The administrator level is recommended.

----End

Result

The loaded configuration script takes effect.

1.3.8 Changing the System Name

This topic describes how to customize the useful system name to differentiate MA5600T/MA5603T/MA5608Ts. This facilitates the management of the MA5600T/MA5603T/MA5608T.

Context

- By default, the system name is device name.
- The system name takes effect immediately after change.
- After the system name is changed, the CLI prompt character changes to the new name accordingly.

Procedure

Step 1 Run the **sysname** command to set the system name.

----End

Result

The CLI prompt character changes to the system name that is set after the command is executed successfully.

Example

To name the first MA5600T/MA5603T/MA5608T at Longgang (a district in Shenzhen, Guangdong, China) **guangdong_shenzhen_longgang_MA5600T/MA5603T/MA5608T_A** based on the rule province_city_district_device name_SN, do as follows:

```
huawei(config)#guangdong_shenzhen_longgang_MA5600T/MA5603T/MA5608T_A
guangdong_shenzhen_longgang_MA5600T/MA5603T/MA5608T_A(config)#
```


Copyright © Huawei Technologies Co., Ltd.

1.3.9 Configuring the System Time

This topic describes how to configure the system time, time zone, time stamp, NTP (Network Time Protocol), and start/end time of the daylight saving time (DST) of the MA5600T/ MA5603T/MA5608T to ensure that they are consistent with those in the actual condition.

Procedure

Step 1 Configure the system time.

Run the **display time** command to query the current system time. If the system time is consistent with the local standard time, you need not change it. If the system time is inconsistent with the local standard time, run the **time** command to change the system time.

Step 2 Configure the system time zone.

Run the **display timezone** command to query the current system time zone. If the system time zone is consistent with the local standard time zone, you need not change it. If the system time zone is inconsistent with the local standard time zone, run the **timezone** command to change the system time zone.

NOTE

- The system time zone include the eastern time zone and the western time zone. "GMT+" indicates the eastern time zone, that is, the local time is ahead of the Greenwich time. "GMT-" indicates the western time zone, that is, the local time is behind the Greenwich time.
- By default, the system time zone is GMT+8:00.

Step 3 Configure the system time stamp.

Run the **display time time-stamp** command to query the time stamp between the NMS and the NE, namely the displayed time format of the SNMP interface. If the system time stamp is consistent with the actual data plan, you need not change it. If the system time stamp is inconsistent with the actual data plan, run the **time time-stamp** command to change the system time stamp.

NOTE

The time type of the SNMP interface between the NMS and the NE are categorized as UTC time and NE local time. By default, the time type is the NE local time.

Step 4 Configure NTP to ensure that the clock of all devices in the network is the same.

- (Optional) Run the **ntp-service refclock-master** command to configure the NTP master clock.
- Run the **ntp-service unicast-server** command to configure the NTP unicast server mode, and specify the IP address of the remote server that functions as the local time server and the interface for transmitting and receiving NTP packets.

Copyright © Huawei Technologies Co., Ltd.

NOTE

- The NTP protocol supports the client/server, peer, broadcast, and multicast working modes. The following uses the client/server mode as an example.
- The L3 interface and the interface IP address must be available for the client and the server to communicate with each other.
- In the client/server mode, you need to configure only the client and the NTP master clock of the server.
- In the client/server mode, the client is synchronized to the server but the server will not be synchronized to the client.
- The clock stratum of the synchronizing device must be smaller than that of the synchronized device. Otherwise, the clock synchronization fails.
- The device that runs the NTP protocol can be synchronized to other clock sources or function as the clock source for synchronizing other clocks. In addition, this device and other devices can be set to synchronized from each other. When the device works in the client mode, you need not set the system time and the device is automatically synchronized to the remote server.

Step 5 Configure the start/end time of the DST.

Run the **display time dst** command to query the current start/end time of the DST of the system. If the start/end time of the DST is consistent with the actual start/end time of the DST, you need not change it. If the start/end time of the DST is inconsistent with the actual start/end time of the DST, run the **time dst** command to change the start/end time of the DST.

----End

Result

The system time, time zone, time stamp, NTP, and start/end time of the DST are consistent with those in the actual condition.

Example

To set the time stamp between the NMS and the NE to use the UTC time, do as follows:

```
huawei#time time-stamp
{ local<K>|utc<K> }:utc

  Command:
          time time-stamp utc
```

Assume that the current time zone of MA5600T/MA5603T/MA5608T A is GMT+7:00, the device uses the network clock to adjust the time, and VLAN interface 2 is used to sent a clock synchronization request packet to MA5600T/MA5603T/MA5608T B (the IP address is 10.20.20.20/24 and the device works at layer 4) that functions as the NTP server. The start time is 00:00:00 on May 1, the end time is 00:00:00 on September 30, and the adjust time is 1:00. That is, if the local time is 5:00, the time is adjusted to 6:00. To set the DST, do as follows:

```
huawei(config)A#timezone GMT+ 7:00
huawei(config)B#ntp-service refclock-master 4
huawei(config)A#ntp-service unicast-server 10.20.20.20 source-interface vlanif 2
huawei(config)A#time dst start 5-1 00:00:00 end 9-30 00:00:00 adjust 1:00
```

Assume that the current time zone of MA5600T/MA5603T/MA5608T A is GMT- 4:00, the local time is used, the current time is 2010-01-01 12:10:10. The start time is 00:00:00 on May 1, the end time is 00:00:00 on September 30, and the adjust time is 2:00. That is, if the local time is 5:00, the time is adjusted to 7:00. To set the DST, do as follows:

```
huawei(config)A#timezone GMT- 4:00
```


Copyright © Huawei Technologies Co., Ltd.

```
huawei(config)A#time 2010-01-01 12:10:10
huawei(config)A#time dst start 5-1 00:00:00 end 9-30 00:00:00 adjust 2:00
```

1.3.10 Configuring a System User

For logging in to, configuring, and managing the MA5600T/MA5603T/MA5608T, system users of different attributes need to be added. This topic describes how to add a system user and modify the user attributes.

1.3.10.1 Adding a System User

This topic describes how to add system users of different attributes for logging in to, configuring, and managing the MA5600T/MA5603T/MA5608T. This facilitates the management of the MA5600T/MA5603T/MA5608T.

Prerequisites

You must have the administrator authority or higher authority.

Context

- The super user and the administrator have the authority to add a user at a lower level, that is:
  - The super user can add an administrator, an operator, or a common user.
  - The administrator can add only an operator or a common user.
- By default, the system has a super user with the name of root and password of admin. The super user cannot be added or deleted. To enhance system security, run the terminal user password command to change the password to meet the requirement after the first successful login. It is recommended that you change the password periodically.
- The user name must be unique, and cannot be **all** or **online**.
- The super user and the administrator can add multiple users consecutively. Up to 127 (total 128 including the root user) users can be added to the system.
- The terminal session max-number command is used to set the maximum number of users who are permitted to log in through the CLI at a time. The default value is 22.

When adding a user, you must configure the user attributes, including the user account, password, profile, authority, permitted reenter number, and appended information. **Table 1-20** lists the user attributes.

Table 1-20 User attributes

User Attribute	Description
Account	An account is also called a user name and consists of 6-15 printable characters. The user name is unique in the system. It cannot contain any space and is case insensitive.
Password	A password consists of 6-15 characters. It must contain at least one digit and one letter, and is case-sensitive.

Copyright © Huawei Technologies Co., Ltd.

User Attribute	Description
User profile	The name of a user profile consists of 1-15 printable characters. A user profile includes the validity period of the user name, validity period of the password, login time, and logout time.

Authority	Users are classified into three levels: common user, operator, and administrator.
	NOTE
	According to the operation authority, users of the MA5600T/MA5603T/MA5608T are classified into four levels: common user, operator, administrator, and super user. The user at one level can add only the user at a lower level. The following lists the authority of all users.
	● Common users can perform basic system operations and simple query operations.
	● Operators can configure the device and the services.
	● For the administrator and the super user, they have the following similarities and differences:
	  ● Similarities:
	  ● Perform all configurations.
	  ● Maintain and manage the device, user account, and user authority.
	  ● Differences:
	  ● Only one super user exists in the system; however, multiple administrators can coexist in the system.
	  ● The super user can add an administrator, but an administrator has no authority to add the super user.

Permitted reenter number	The permitted reenter number determines whether a user name can be used to log in to the system from several terminals at the same time. The permitted reenter number ranges from 0 to 4, and is generally set to 1.
Appended information	Appended information is a type of additional information about the user. It consists of a string of 0-30 characters. It can be the telephone number or the address of a user.

Procedure

Step 1 Run the **terminal user name** command to add a user that is consistent with the actual data plan.

Step 2 Run the **display terminal user** command to query the user information.

----End

Result

The queried user information is the same as the actual data plan.

Copyright © Huawei Technologies Co., Ltd.

Example

With the administrator authority, to add a common user with the account as **huawei**, password as **test01**, user profile as the default **root** user profile, user level as **Common User**, permitted reenter number as **3**, and appended information as **user**, do as follows:

```
huawei(config)#terminal user name
  User Name(length<6,15>):huawei
  User Password(length<6,15>):test01//The password is not displayed on the
console.
  Confirm Password(length<6,15>):test01//The password is not displayed on the
console.
  User profile name(<=15 chars)[root]:
  User's Level:
     1. Common User  2. Operator:1
  Permitted Reenter Number(0--4):3
  User's Appended Info(<=30 chars):user
  Adding user succeeds
  Repeat this operation? (y/n)[n]:n

huawei(config)#display terminal user name huawei
------------------------------------------------------------------------------
  Name            Level    Status  Reenter Profile         Append
                                   Num                     Info
  ------------------------------------------------------------------------------
  huawei          User     Offline       3 root            user
  ------------------------------------------------------------------------------
```

1.3.10.2 Modifying the System User Attributes

This topic describes how to modify the attributes of a system user, including the password, user profile, authority, permitted reenter number, and appended information in the case that the user attributes are not consistent with the current data plan.

Prerequisites

For details about the user authority, see "Context".

Context

Table 1-21 lists the user attributes that can be modified and the related restrictions.

Table 1-21 Modifying the user attributes

User Attribute	Restriction
Password	● The super user and the administrator can change their own passwords and the passwords of users at lower levels. When changing the password of a user at a lower level, the super user and the administrator need not input the old password. ● The common user and the operator can change only their own passwords, but they must input their old passwords for this purpose.

Copyright © Huawei Technologies Co., Ltd.

User Attribute	Restriction
User profile	● The super user and the administrator can modify the profiles bound to them and the profiles bound to users at lower levels. ● The user name and the password must meet the specifications described in the user profile to be bound. Otherwise, the binding operation fails.
Authority	The super user and the administrator can modify the authority of users at lower levels. In addition, the super user and the administrator can modify the user authority only to a level lower than them.
Permitted reenter number	● The super user and the administrator can change the permitted reenter number of a user at a lower level. ● The permitted reenter number of the super user cannot be changed.
Appended information	● The super user and the administrator can modify their own appended information and the appended information about users at lower levels. ● The common user and the operator can modify only their own appended information.

Procedure

Step 1 Modify the system user attributes.

NOTE

Before modifying the user attributes, run the **display terminal user** command to query the user attributes to be modified.

- Run the **terminal user password** command to change the password of a user.

  The password of a user consists of 6-15 characters, in which at least one digit and one letter must be contained. The password is case sensitive.
- Run the **terminal user user-profile** command to modify the profile bound to a user.
- Run the **terminal user level** command to modify the authority of a user.
- Run the **terminal user reenter** command to change the permitted reenter number of a user.
- Run the **terminal user apdinfo** command to modify the appended information about a user.

  When the system has any problem, you can contact the user after querying the user appended information. It is recommended that the user appended information be modified into the information that has the actual meaning, such as the contact means and the user address.

Step 2 Check the user information.

Run the **display terminal user** command to query the user information.

----End

Copyright © Huawei Technologies Co., Ltd.

Result

The queried user information is consistent with the user attributes that are modified, and login to the MA5600T/MA5603T/MA5608T by using the original user name and password is successful.

Example

To modify the attributes of user **huawei**, including changing the password to **test02**, user profile to operator profile, user level to **operator**, permitted reenter number to **4**, and appended information to **operator**, do as follows:

```
huawei(config)#terminal user password
  User Name(<=15 chars):huawei
  New Password(length<6,15>):test02//The password is not displayed on the console.
  Confirm Password(length<6,15>):test02//The password is not displayed on the
console.
  Information takes effect
  Repeat this operation? (y/n)[n]:n

huawei(config)#terminal user user-profile
  User Name(<=15 chars):huawei
  Permitted user-profile[root]:operator
  Confirm user-profile:operator
  Configuration will take effect when the user logs on next time.
  Repeat this operation? (y/n)[n]:n

huawei(config)#terminal user level
  User Name(<=15 chars):huawei
     1. Common User  2. Operator:
  User's Level:2
  Confirm Level:2
  Information will take effect when this user logs on next time
  Repeat this operation? (y/n)[n]:n

huawei(config)#terminal user reenter
  User Name(<=15 chars):huawei
  Permitted Reenter Number(0--4):4
  Confirm Reenter Number(0--4):4
  Information will take effect when this user logs on next time
  Repeat this operation? (y/n)[n]:n

huawei(config)#terminal user apdinfo
  User Name(<=15 chars):huawei
  User's Appended Info(<=30 chars):operator
  Information takes effect
  Repeat this operation? (y/n)[n]:n

huawei(config)#display terminal user name huawei
  ------------------------------------------------------------------------------
  Name            Level    Status  Reenter Profile         Append
                                   Num                     Info
  ------------------------------------------------------------------------------
  huawei          Operator Offline       4 operator        operator
  ------------------------------------------------------------------------------
```

1.3.11 Configuring a Board

Specific services require specific boards. To use a board, you need to first confirm the automatically discovered board or add the board offline.

Copyright © Huawei Technologies Co., Ltd.

1.3.11.1 Adding a Board Offline

This topic describes how to add a board to an idle slot that is consistent with the board actually planned beforehand to ensure that the board runs immediately the board is installed in the slot.

Prerequisites

The slot to which a board is added must be idle.

Context

- The boards other than the control board can be added offline.
- After a board is added offline, the board status is displayed as **Failed**. The board status becomes normal only when a board of the same type as the board added offline is installed in the slot. If a board of a different type is installed, the board resets repeatedly due to the board type mismatch.

Procedure

Step 1 Run the **board add** command to add a board offline.

NOTE

- The shelf ID and the slot ID of the board added offline must be the same as the actual position. Otherwise, when the board is installed, the board status cannot be changed to normal.
- The type of the board added offline must be the same as the type of the board installed. Otherwise, when the board is installed, the board status cannot be changed to normal.

Step 2 Run the **display board** *frameid [/slotid]* command to query the type of the added board.

----End

Result

The type of the added board is the same as the board type that is planned. When a board is installed in the slot in which the board is added, the board status is displayed as **Normal**.

Example

To add a service board GPBD offline in slot 0/2, do as follows:

```
huawei(config)#board add 0/2 h802gpbd
  0 frame 2 slot board added successfully

huawei(config)#display board 0/2

  ---------------------------------------
  Board Name          : H802GPBD
  Board Status        : Failed
  ---------------------------------------

  -------------------------------------------------------------
    Port   Port   min-distance   max-distance   Optical-module
           type       (km)           (km)           status
  -------------------------------------------------------------
    0      GPON        0              20               -
    1      GPON        0              20               -
    2      GPON        0              20               -
    3      GPON        0              20               -
    4      GPON        0              20               -
```


Copyright © Huawei Technologies Co., Ltd.

```
  5     GPON        0             20               -
  6     GPON        0             20               -
  7     GPON        0             20               -
 ------------------------------------------------------------
 In port 0, the total of ONTs are: 0
 In port 1, the total of ONTs are: 0
 In port 2, the total of ONTs are: 0
 In port 3, the total of ONTs are: 0
 In port 4, the total of ONTs are: 0
 In port 5, the total of ONTs are: 0
 In port 6, the total of ONTs are: 0
 In port 7, the total of ONTs are: 0
```

1.3.11.2 Confirming a Board

This topic describes how to confirm a board after the board installed in an idle slot is automatically discovered. This ensures that the auto-discovered board runs in the normal state.

Prerequisites

A board must be installed in an idle slot or all the boards in the shelf must be installed. After that, the system automatically identifies the board type, and the board status is **Auto_find**.

Procedure

Step 1 Run the **board confirm** command to confirm an **Auto_find** board.

NOTE

- To confirm only one board, run the **board confirm** *frameid/slotid* command.
- To confirm all the boards in a shelf, run the **board confirm** *frameid* command.

Step 2 Run the **display board** *frameid [/slotid]* command to query the board status.

----End

Result

The board status is displayed as **Normal**.

Example

To confirm the service board in slot 0/2, do as follows:

```
huawei(config)#board confirm 0/2
  0 frame 2 slot board confirms successfully

huawei(config)#display board 0/2

 ----------------------------------------
  Board Name          : ADL
  Board Status        : Normal
  ----------------------------------------

  ------------------------------------------------------------------------------
  Port    Port Type   Port Status      Line Profile  Alarm Profile  Ext Profile
  ------------------------------------------------------------------------------
     0    ADSL        Activating          1002              1           --
     1    ADSL        Activating          1002              1           --
     2    ADSL        Activating          1002              1           --
     3    ADSL        Activating          1002              1           --
     4    ADSL        Activating          1002              1           --
```


Copyright © Huawei Technologies Co., Ltd.

```
     5    ADSL        Activating          1002              1           --
     6    ADSL        Activating          1002              1           --
     7    ADSL        Activating          1002              1           --
     8    ADSL        Activating          1002              1           --
     9    ADSL        Activating          1002              1           --
    10    ADSL        Activating          1002              1           --
    11    ADSL        Activating          1002              1           --
    12    ADSL        Activating          1002              1           --
    13    ADSL        Activating          1002              1           --
    14    ADSL        Activating          1002              1           --
---- More ( Press 'Q' to break ) ----
```

1.3.11.3 Checking the Board Status

This topic describes how to check whether the board works in the normal state.

Procedure

Step 1 Run the **display board** *frameid* command to query the status of all the boards.

----End

Result

All the boards work in the normal state. That is, all of the service board status is displayed as **Normal**, the active control board status is displayed as **Active_normal**, and the standby control board status is displayed as **Standby_normal**.

Example

To query the information about all the boards of shelf 0, do as follows:

```
huawei(config)#display board 0
  ------------------------------------------------------------------------------
  SlotID  BoardName  Status         SubType0 SubType1    Online/Offline
  ------------------------------------------------------------------------------
  0
  1
  2
  3
  4       H802GPBD   Normal
  5
  6       H802GPBD   Normal
  7
  8
  9       H801SCUL   Active_normal  FLBA
  10
  11
  12      H802GPBD   Normal
  13
  14      H802GPBD   Normal
  15
  16
  17      H802GPBD   Normal
  18
  19      H801GICG   Normal
  20
  21
  22
  ------------------------------------------------------------------------------
```


Copyright © Huawei Technologies Co., Ltd.

1.3.12 Checking the Status of the Upstream Port

This topic describes how to check whether the upstream port is in the normal state.

Procedure

Step 1 Follow the steps below to check the status of the upstream port.

- If the control board is adopted for upstream transmission, do as follows:
  1. For the MCU control board, run the **interface mcu** command to enter the MCU mode. For other control boards, run the **interface scu** command to enter the SCU mode.
  2. Run the **display port state all** command to check whether the upstream port is in the normal state.
- If the upstream board is adopted for upstream transmission, do as follows:
  1. Run the **interface giu** command to enter the GIU mode.
  2. Run the **display port state all** command to check whether the upstream port is in the normal state.

----End

Result

The upstream port is in the normal state. That is, the upstream port is in the **active** state and the link is in the **online** state. If the optical port is adopted for upstream transmission, **Optic Status** is displayed as **normal**.

1.3.13 Checking the Status of the Service Port

This topic describes how to check whether the service port is in the normal state.

Prerequisites

NOTE

The MA5600T/MA5603T/MA5608T provides various service ports. The following only describes how to check the status of an ADSL2+ port and a GPON port.

Procedure

Step 1 Follow the steps below to check the status of the service port.

- If the user port is an ADSL2+ port:
  1. Run the **interface adsl** command to enter the ADSL mode.
  2. Run the **display port state** command to check whether the service port is in the normal state.
- If the user port is a GPON port:
  1. Run the **interface gpon** command to enter the GPON mode.
  2. Run the **display port state** command to check whether the service port is in the normal state.

----End

Copyright © Huawei Technologies Co., Ltd.

Result

All the service ports are in the normal state. That is :

- If the user port is an ADSL2+ port: **Status** is displayed as **Activated**.
- If the user port is a GPON port: **Status** is displayed as **Activated**, and **Laser state** is displayed as **Normal**.

1.3.14 Enabling the ONT Automatic Discovery function

After the ONT automatic discovery function is enabled, online ONTs can be automatically displayed on the OLT.

Procedure

Step 1 Run the **port *portid* ont-auto-find** command to enable the auto discovery function of the ONT.

Step 2 Run the **port fec(gpon)**command to enable the forward error correction (FEC) function.

NOTE

Only GPON supports this operation.

----End

Result

Run the **display port info(gpon)** command to query the configuration.

```
huawei(config-if-gpon-0/3)#display port info
{ portid<U><0,7> }:0

  Command:
          display port info 0
  ------------------------------------------------------
  F/S/P                                     0/3/0
  Min distance(km)                          0
  Max distance(km)                          20
  Left guaranteed bandwidth(kbps)           1240576
  Number of T-CONTs                         0
  Autofind                                  Enable
  FEC check                                 Enable
  Laser switch                              On
  ONT encryption key switching interval(m)  Disable
  ------------------------------------------------------
```

1.3.15 Testing the Optical Power of an Optical Port

This topic describes how to check whether the optical signal transmit and receive modules are normal by testing the mean launched power and the actual input power.

1.3.15.1 Measuring the Transmit Optical Power of an OLT PON Port

Check whether the optical module on a PON port of the OLT works properly by measuring the transmit optical power.

Prerequisites

- The OLT is powered on.

Copyright © Huawei Technologies Co., Ltd.

- The PON board is in the normal state.
- The PON port is enabled.

Tools, Meters and Materials

- Single-mode fiber jumper with the SC/PC connector. No longer than 1 m. Best to use new jumper.
- Burst optical power meter or ordinary optical power meter.

Impact on the System

When the transmit optical power of a PON port on the OLT is measured, the PON port will fail to transmit any service.

Precautions

DANGER

Do not look into the optical port or the optical fiber connector without eye protection.

Before or after measuring the optical power, you need to clean the connector of the optical fiber. This is because if a contaminated optical fiber is connected to a normal optical fiber connector, the connector will be contaminated, which leads to abnormal attenuation and reflection and thus affecting optical path quality.

Procedure

Step 1 Configuring the measure parameters of the optical power meter.

- Unit of optical power: dBm
- Wavelength: 1490 nm

Step 2 Connect the optical power meter directly to the optical module on the OLT PON port using optical fiber jumper, as shown in **Figure 1-45**. The value on the optical power meter is the transmit optical power of the OLT PON port.

Figure 1-45 Measuring the Transmit Optical Power of an OLT PON Port

Copyright © Huawei Technologies Co., Ltd.

NOTE

- If the value on the optical power meter changes within a range of 0.2 dBm, take the average value.
- If the value on the optical power meter changes in a range wider than 0.2 dBm, then it is possible that the fiber is not properly connected, the fiber is excessively bent, or the fiber connector has dust.
- Do not bend the fiber. A bent fiber may affect the test result.

Step 3 Compare the test result with the optical module parameters of the corresponding board in the hardware description.

----End

Result

- If the test result is between the maximum and minimum output optical power of the optical module of the board, it indicates that the optical module works properly.
- If the test result is no between the maximum and minimum output optical power of the optical module of the board, it indicates that the optical module does not work properly.

1.3.15.2 Measuring the Receive Optical Power of an OLT PON Port

Determine whether there are continuous mode ONUs or rogue ONUs by measuring the optical power of the OLT PON port.

Prerequisites

- The ONU is powered on.
- The ONU PON port is enabled.
- The optical fiber between the OLT and the ONU is properly connected.

Tools, Meters and Materials

Burst optical power meter

Impact on System

When the receive optical power of a PON port on the OLT is measured, corresponding PON port will fail to transmit any service.

Precautions

DANGER

Do not look into the optical port or the optical fiber connector without eye protection.

Before or after measuring the optical power, you need to clean the connector of the optical fiber. This is because if a contaminated optical fiber is connected to a normal optical fiber connector, the connector will be contaminated, which leads to abnormal attenuation and reflection and thus affecting optical path quality.

Copyright © Huawei Technologies Co., Ltd.

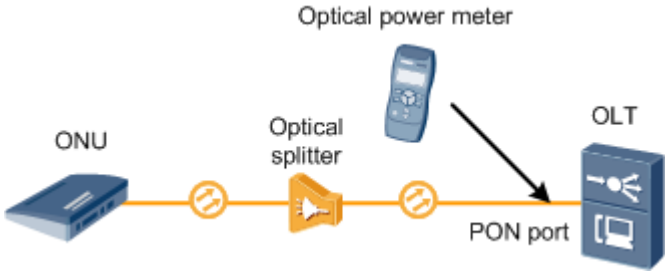
Procedure

Step 1 Configuring the measure parameters of the optical power meter.

- Unit of optical power: dBm
- Wavelength: 1310 nm

Step 2 Remove the fiber from the OLT PON port and connect it to the optical power meter, as shown in **Figure 1-46**.

Figure 1-46 Measuring the Receive Optical Power of an OLT PON Port



Step 3 Wait for 10s and read the value. Check the value on the optical power meter for one minute.

Step 4 After measuring the transmit optical power, insert the optical fiber removed in step 2 to restore the connection between the ONU and the OLT.

----End

Result

- If no value can be read or the value is lower than -40 dBm on the optical power meter, there is no rogue ONU or continuous mode ONU connected to the PON port.
- If a value can always be read and is higher than -28 dBm on the optical power meter, there are ONUs in continuous mode connected to the PON port.
- If a value can be read at one time and cannot be read at another time and the value is higher than -28 dBm, there are rogue ONUs connected to the PON port (that is, an ONU that transmits data in the timeslot that is not allocated by the OLT to it).

1.3.15.3 Measuring the Transmit Optical Power of an ONU PON Port

Measuring the transmit optical power of a PON port on the ONU helps you check whether the optical module of the PON port functions properly and whether the ONU is a continuous-mode ONU or a rogue ONU.

Prerequisites

- The ONU is powered on.
- The PON port is enabled.

Copyright © Huawei Technologies Co., Ltd.

Tools and Meters

- Single-mode optical jumper no longer than 1 m whose connector matches the ONU's interface specifications. A new jumper is recommended.
- Burst optical power meter

Impact on the System

When the transmit optical power of a PON port on the ONU is measured, the PON port is not able to carry any service.

Precautions

DANGER

Do not look into the optical port or the optical fiber connector without eye protection.

Before or after measuring the optical power, you need to clean the connector of the optical fiber. This is because if a contaminated optical fiber is connected to a normal optical fiber connector, the connector will be contaminated, which leads to abnormal attenuation and reflection and thus affecting optical path quality.

Procedure

Step 1 Configure the measuring parameters of the optical power meter.

- Optical power unit: dBm
- Wavelength (nm): 1310

Step 2 Remove all optical fibers connected to the PON ports on the ONU and ensure that the ONU is not connected to any optical splitters or OLTs.

NOTE

When certain ONUs support network protection in the case that multiple PON ports are used for upstream transmission, you need to remove all the optical cables of the ONU PON ports. This is because the continuous mode of the ONU needs to be enabled when you measure the ONU transmit power. If the ONU is connected to a splitter or OLT, the other ONUs that are connected to the same PON port fail to go online.

Step 3 Connect the optical power meter directly to the optical module on the ONU PON port using an optical jumper, as shown in **Figure 1-47**.

Figure 1-47 Measuring the transmit optical power of an ONU PON port

Step 4 Wait 10s and then read the value. Check the value on the optical power meter in one minute.

Copyright © Huawei Technologies Co., Ltd.

Step 5 Enable the continuous-mode ONU function. The value read on the optical power meter is the transmit optical power of the ONU PON port. Compare the result as tested with the PON optical module parameter in the ONU product manual.

NOTE

- Generally, an ONU does no transmit optical signals when it is not connected to the OLT. In this case, enable the continuous-mode ONU function to make the ONU transmit optical signals. For how to enable the continuous-mode ONU function, see the ONU product manual.
- If the value on the optical power meter changes within a range of 0.2 dBm, take the average value.
- If the value on the optical power meter changes in a range wider than 0.2 dBm, there is a probability that the optical fiber is not properly connected, the optical fiber is excessively bent, or the optical fiber connector is not clean.
- Do not bend the optical fiber. A bent optical fiber may affect the test result.

Step 6 After measuring the transmit optical power, disable the continuous-mode ONU function.

NOTE

After measuring the transmit optical power, you must disable the continuous-mode ONU function. Otherwise, other ONUs cannot go online after the ONU is connected to the OLT.

Step 7 Insert the optical fiber removed in step 1 to restore the connection between the ONU and the OLT.

----End

Result

- The test result in step 4 helps to determine whether the ONU is a continuous-mode ONU or a rogue ONU.
  - If no value can be read or the value is smaller than -40 dBm on the optical power meter, there is no rogue ONU or continuous-mode ONU connected to the PON port.
  - If a value can always be read and is larger than -28 dBm on the optical power meter, there are continuous-mode ONUs connected to the PON port.
  - If a value can be read at one time and cannot be read at another time and the value is larger than -28 dBm, there are rogue ONUs (that is, ONUs that transmit data in the timeslot that is not allocated by the OLT to them) connected to the PON port.
- The test result in step 5 helps to determine whether the optical module of the PON port on the ONU works properly.
  - If the test result is between the maximum and minimum output optical power of the ONU optical module, the optical module works properly.
  - If the test result is not between the maximum and minimum output optical power of the ONU optical module, the optical module does not work properly.

1.3.15.4 Measuring the Receive Optical Power of an ONU PON Port

Measuring the receive optical power of an ONU PON port helps to check the optical path quality.

Prerequisites

- The OLT is powered on.
- The OLT PON port is enabled.

Copyright © Huawei Technologies Co., Ltd.

- The optical fiber between the OLT and the ONU is properly connected.

Tools and Meters

Burst optical power meter or ordinary optical power meter

Impact on the System

When the receive optical power of a PON port on the ONU is measured, the PON port is not able to carry any service.

Precautions

DANGER

Do not look into the optical port or the optical fiber connector without eye protection.

Before or after measuring the optical power, you need to clean the connector of the optical fiber. This is because if a contaminated optical fiber is connected to a normal optical fiber connector, the connector will be contaminated, which leads to abnormal attenuation and reflection and thus affecting optical path quality.

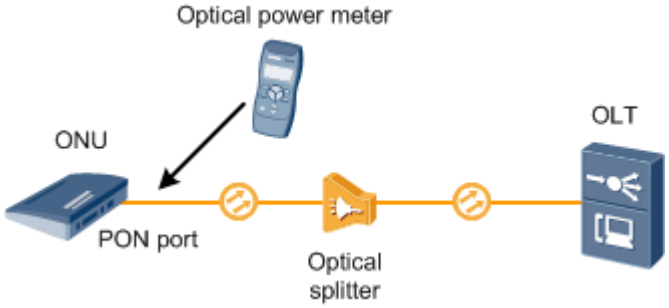
Procedure

Step 1 Configure the measuring parameters of the optical power meter.

- Optical power unit: dBm
- Wavelength (nm): 1490

Step 2 Remove the optical fiber from the ONU PON port and connect it to the optical power meter, as shown in **Figure 1-48**. The value read on the optical power meter is the receive optical power of the ONU PON port.

Figure 1-48 Measuring the Receive Optical Power of an ONU PON Port



Copyright © Huawei Technologies Co., Ltd.

NOTE

- If the value on the optical power meter changes within a range of 0.2 dBm, take the average value.
- If the value on the optical power meter changes in a range wider than 0.2 dBm, there is a probability that the optical fiber is not properly connected, the optical fiber is excessively bent, or the optical fiber connector is not clean.
- Do not bend the optical fiber. A bent optical fiber may affect the test result.

----End

Result

Compare the result as tested with the theoretical value of the ONU receive optical power in the ODN plan. If the difference between the actual value and the theoretical value is larger than 2 dBm, the line may be faulty.

NOTE

Generally, the normal range of the receive optical power of a GPON port on the ONU is from -27 dBm to -8 dBm.

1.3.16 Commissioning the EMU

The MA5600T/MA5603T/MA5608T monitors various environment parameters (including the temperature, humidity, and voltage of the power supply) to ensure that the MA5600T/MA5603T/MA5608T can work stably in a proper environment. This topic describes how to commission the environment monitoring unit (EMU).

1.3.16.1 Environment Monitoring Application

This topic describes the environment monitoring applications in different cabinets.

Table 1-22 lists the environment monitoring applications in different cabinets.

Table 1-22 Environment monitoring applications in different cabinets

Monitoring Solution	Cabinet Type	Typical Configuration
H801ESC Monitoring Solution	N63E-22	● Two MA5600T shelves ● One MA5600T shelf + one SPL shelf
ESCM Monitoring Solution	-	Use this program when you need to monitor the ESCM
EPS75-4815AF Monitoring Solution (PMIB01)	F01D500	One MA5600T(MA5603T) shelf
EPS30-4815AF Monitoring Solution (PMIB01)	F01S300	One MA5603T shelf
GEPS4845 Monitoring Solution	F01D500	One MA5600T(MA5603T) shelf

Copyright © Huawei Technologies Co., Ltd.

Monitoring Solution	Cabinet Type	Typical Configuration
ETP4830 Monitoring Solution	F01S300	One MA5603T shelf
ETP4890 Monitoring Solution	F01D500	One MA5600T(MA5603T) shelf
ETP48150 Monitoring Solution	F01D2000	Two MA5600T(MA5603T) shelves
Power3000 Monitoring Solution	-	Use this program when you need to monitor the external power supply Power 3000
Heat Exchanger Monitoring Solution	-	Heat Exchanger
Fan Tray Monitoring Solution	-	Fan Tray

1.3.16.2 Commissioning the EMU_ESC

This topic describes how to commission the H801ESC board to ensure that it monitors the environmental conditions of the device according to the actual conditions.

Context

ESC stands for the environment and power monitoring board. The H801ESC board monitors environment parameters such as temperature, humidity, smoke, water, fire, voltage, and power supply through various sensors.

When commissioning the H801ESC board, pay attention to the following points:

- The EMU sub-nodes are numbered from 0 to 31.
- When the system is configured with multiple EMUs simultaneously, make sure that the sub-nodes do not conflict with each other.

Table 1-23 lists the default configuration of the H801ESC board.

Table 1-23 Default configuration of the H801ESC board

Parameter	Default Value
Sub-node	15

Copyright © Huawei Technologies Co., Ltd.

Parameter	Default Value
Analog parameters	ESC analog parameter IDs: ● 0: allocated to the board temperature sensor by default (unable to be changed by the user). ● 1-4: allocated to the voltage sensor by default. – 1 indicates -48 V input of channel 0. – 2 indicates -48 V input of channel 1. – 3 indicates -48 V input of channel 2. – 4 indicates -48 V input of channel 3. ● 5-8: user-defined analog parameters allocated to other extended analog sensors, such as the temperature sensor and the humidity sensor.
	Upper and lower alarm thresholds ● Temperature: 5°C to 55°C ● Humidity: 0% RH to 80% RH
Digital parameters	ESC digital parameter IDs ● Allocated by default (unable to be changed by the user) – 0: MDF – 1: door status sensor 0 – 9: water – 10-13: lightning arresters 0-3 – 14-15: switches 11 and 12 – 16-17: switches 21 and 22 – 18-19: switches 31 and 32 – 20-21: switches 41 and 42 – 22: external sensor power ● User-defined IDs – 2-8: allocated to other extended digital sensors.

Procedure

Step 1 Set the DIP switch of the sub-node for the H801ESC board. By default, the sub-node ID is 15.

The H801ESC board communicates with the MA5600T/MA5603T/MA5608T in the master node and sub-node mode. Therefore, the DIP switch of the sub-node for the H801ESC board must be consistent with that for the MA5600T/MA5603T/MA5608T. For details about how to configure the DIP switches of the H801ESC board, see the Description of DIP Switches in **1.3.1.1 Checking the Settings of DIP Switches on the H801ESC Board**.

Step 2 Insert the H801ESC board into the corresponding slot of the PDU, and make sure that the MA5600T/MA5603T/MA5608T and the H801ESC board are connected through the RS-485 serial port cable.

Copyright © Huawei Technologies Co., Ltd.

When the device is delivered, the H801ESC board is correctly connected to the shelf. The connection need not be changed for the device commissioning. The COM2 of the H801ESC board is connected to the ESC of the MA5600T/MA5603T/MA5608T. In this case, the H801ESC collects and reports the environment information to the control board.

Step 3 Run the **emu add** command to add an H801ESC board. By default, the sub-node ID is 15.

Step 4 Run the **interface emu** command to enter the H801ESC mode.

Step 5 Run the **esc analog** command to configure the ESC analog parameters. By default, the upper and lower alarm thresholds of the temperature are 55°C and 5°C respectively; the upper and lower alarm thresholds of the humidity are 80% RH and 0% RH respectively.

Step 6 Run the **esc digital** command to set the ESC digital parameters.

Step 7 Run the **save** command to save the data.

----End

Result

- In step 2, you can confirm that the RUN ALM LED on the H801ESC board is orange and blinks repeatedly once in every 300 ms, which indicates that the board is registering.
- After a while, the RUN ALM LED on the H801ESC board turns orange and is on for 1s and off for 1s repeatedly, which indicates that an alarm is generated. Certain EMU parameters have the initial configurations (namely, default alarm thresholds); therefore, if any parameter reaches the threshold, an alarm is generated.
- After the configuration, the RUN ALM LED on the H801ESC board turns green and is on for 1s and off for 1s repeatedly, which indicates that the H801ESC board monitors the environment normally.
- In the H801ESC mode, run the **display esc system parameter** command to check whether the ESC information is the same as the data plan.
- Close doors of the cabinet, and query alarms. Ensure that no alarm of the monitoring parameters is generated.

Example

Add an H801ESC board, set the analog and digital parameters of the H801ESC board, and save the data.

To set the ESC analog parameters (set the user-defined analog parameter ID to 5, upper alarm threshold to 70, lower alarm threshold to -30, analog parameter name to Temperature_1 with the unit of C) and the ESC digital parameters (set the user-defined digital parameter ID to 7, set the door status alarm whose ID is 8, set the alarm name to Door_1 and the available level of the alarm to high level), do as follows:

```
huawei(config)#emu add 1 H801ESC 0 15 H801ESC
huawei(config)#interface emu 1
huawei(config-if-h801esc-1)#esc analog 5 alarm-upper-limit 70 alarm-lower-limit
-30 name Temperature_1 unit C
huawei(config-if-h801esc-1)#esc digital 7 digital-alarm 8 name Door_1 available-
level high-level
huawei(config-if-h801esc-1)#display esc system parameter
huawei(config-if-h801esc-1)#quit
huawei(config)#save
```


Copyright © Huawei Technologies Co., Ltd.

1.3.16.3 Configuring H801VESC Environment Monitoring Parameters

The MA5608T can monitor the environment status through its built-in virtual environment monitoring unit (EMU) H801VESC. This topic describes how to configure the H801VESC.

Context

- The H801VESC is a built-in virtual EMU of the control board on the MA5608T, and the ALARM port on the control board is connected to the external sensor through an environment monitoring cable.
- You need to manually add the H801VESC. The recommended subnode ID is 25.
- The H801VESC supports seven digital parameters, all of which can be defined by users. In an F01S200 cabinet, only four digital parameters are used.
- By default, the valid levels of default digital parameters are all high levels.

Procedure

Step 1 Add the H801VESC.

Run the **emu add** command to add the H801VESC.

Step 2 Query the status of the H801VESC.

Run the **display emu** command to query the status of the H801VESC. Ensure that it is running properly.

Step 3 Configure the digital parameters.

Run the **interface emu** command to enter the EMU mode.

Run the **vesc digital**command to configure the valid level, name, and alarm ID of the digital parameters.

Step 4 Query the environment information about the H801VESC.

Run the **display vesc environment info** command to query the environment information about the H801VESC.

Step 5 Run the **save** command to save the data.

----End

Result

After the configuration, the H801VESC works in the normal state and monitors the digital parameters set on the MA5608T. When the actual level of a monitored digital parameter is different from the valid level preset in the system, the MA5608T reports an alarm.

Example

To configure the H801VESC of the MA5608T in an F01S200 cabinet, do as follows (**Table 1-24** lists the data plan for configuring the H801VESC of the MA5608T in the F01S200 cabinet):

Copyright © Huawei Technologies Co., Ltd.

Table 1-24 Data plan for configuring the H801VESC

Item	Data	Remarks
EMU	EMU ID: 2 Subnode ID: 25	The ID and subnode ID of the H801VESC cannot conflict with those of the existing EMUs.
Digital parameters	Digital parameter ID: 0	-
	Valid level of digital parameter 0: low level	When the low level represents the valid level, the MA5608T does not report an alarm in the case of low level.
	Name of digital parameter 0: Temperature	This digital parameter is set according to the actual requirements. The monitoring digital parameter of the temperature sensor is set to monitor the temperature.
	Digital parameter ID: 1	-
	Valid level of digital parameter 1: low level	When the low level represents the valid level, the MA5608T does not report an alarm in the case of low level.
	Name of digital parameter 1: Door	This digital parameter is set according to the actual requirements. The monitoring digital parameter of the door sensor is set to monitor the door status.
	Digital parameter ID: 2	-
	Valid level of digital parameter 2: low level	When the low level represents the valid level, the MA5608T does not report an alarm in the case of low level.
	Name of digital parameter 2: Arrester	This digital parameter is set according to the actual requirements. The monitoring digital parameter of the lightning arrester status sensor is set to monitor the arrester status.
	Digital parameter ID: 3	-
	Valid level of digital parameter 3: low level	hen the low level represents the valid level, the MA5608T does not report an alarm in the case of low level.
	Name of digital parameter 3: Fan	This digital parameter is set according to the actual requirements. The monitoring digital parameter of the fan status sensor is set to monitor the fan status. **NOTE** The enhanced heat dissipation module is an optional module. The fan monitoring digital parameter is required only when the enhanced heat dissipation module is configured. Otherwise, the system will report an alarm.

```
huawei(config)#emu add 2 H801VESC 0 25 H801VESC
huawei(config)#display emu 2
```


Copyright © Huawei Technologies Co., Ltd.

```
  EMU ID: 2
  ------------------------------------------------------------------------------
  EMU name    : H801VESC
  EMU type    : H801VESC
  Used or not : Used
  EMU state   : Normal
  Frame ID    : 0
  Subnode     : 25
  ------------------------------------------------------------------------------
huawei(config)#interface emu 2
huawei(config-if-h801vesc-2)#vesc digital 0 available-level low-level name
Temperature
huawei(config-if-h801vesc-2)#vesc digital 1 available-level low-level name Door
huawei(config-if-h801vesc-2)#vesc digital 2 available-level low-level name
Arrester
huawei(config-if-h801vesc-2)#vesc digital 3 available-level low-level name Fan

huawei(config-if-h801vesc-2)#display vesc environment info
  EMU ID: 2                             VESC environment state
  --------------------------Digital environment info-------------------------
  ID Name                State  Value |ID Name                State  Value
  0  Temperature         Normal 0     |1  Door                Alarm  1
  2  Arrester            Normal 0     |3  Fan                 Normal 0
  4  -                   Normal 1     |5  -                   Normal 1
  6  -                   Normal 1
  ------------------------------------------------------------------------------
huawei(config-if-h801vesc-2)#quit
huawei(config)#save
```

1.3.16.4 Configuring the Environment Monitoring Parameters of the EPS30-4815AF

This topic describes how to configure the environment monitoring parameters of the EPS30-4815AF through the CLI.

Mapping Between Monitoring Parameters and Device Ports

Table 1-25 describes the mapping between the monitoring parameters displayed on the sensor transfer box.

Table 1-25 Mapping between the monitoring parameters displayed on the host and the ports on the sensor transfer box

Monitoring Parameter Displayed on the Host	Device Port
Temperature	TEM-HU
Humidity	TEM-HU
Digital 0	JTD1
Digital 1	JTD2
Digital 2	JTD3
Digital 3	JTD4
Digital 4	JTD5

Copyright © Huawei Technologies Co., Ltd.

Monitoring Parameter Displayed on the Host	Device Port
Digital 5	JTD6
Digital 6	JTD7

NOTE

Before adding a user-defined analog or monitoring digital parameter, make sure that the port corresponding to this parameter is properly connected to an environment monitoring cable.

Configuration Process

The monitoring parameters can be reported to the control system only when the data for the EPS30-4815AF is configured correctly in the system.

Table 1-26 lists the commands used during the configuration.

Table 1-26 Commands for configuring the EPS30-4815AF

To...	Run the Command...
Add an EMU	**emu add**
Query the configuration parameters of the power system	**display power system parameter**
Query the power environment parameters	**display power environment parameter**
Query the alarm information of the power supply	**display power alarm**
Configure the battery charging parameters	**power charge**
Configure the battery management parameters	**power battery parameter**
Configure the upper/lower temperature alarm limits or the upper/lower temperature test limits	**power battery temperature**
Configure the battery set power-off parameters	**power off**
Configure the power distribution parameters	**power supply-parameter**
Configure the battery discharging test parameters	**power battery-test**

Copyright © Huawei Technologies Co., Ltd.

To...	Run the Command...
Configure the parameters for the power rectifier module	**power module-num**
Configure the battery high-temperature power-off parameters	**power temperature-off**
Configure the environment monitoring parameters	**power environment**
Configure the external extended digital parameters	**power outside-digital**

1. Log in to the device through the maintenance terminal and add an EMU.
2. Query the status of the EPS30-4815AF.
3. Enter the environment monitoring configuration mode and query the default configuration.
4. Configure the battery management parameters.
5. Configure the battery discharging test parameters.
6. Configure the battery high-temperature power-off parameters.
7. Configure the environment parameters.
8. Configure the extended digital parameters.
9. Query the information about the configured parameters and environment parameters of the power system.
10. Query the alarms, and confirm that the door status alarm other than alarms for other monitoring parameters is generated. The door status sensors of the device compartment and the temperature control compartment are in serial connection, and are monitored as a variable.
11. Save the data.
12. Close all doors of the cabinet. Then, query the alarm information again, and confirm that there is no alarm for any monitoring parameter.

Data Plan

In this topic, the application in the F01S300 cabinet is considered as an example. **Table 1-27** provides the data plan for configuring the monitoring parameters of the EPS30-4815AF.

Copyright © Huawei Technologies Co., Ltd.

Table 1-27 Data plan for configuring the monitoring parameters of the EPS30-4815AF

Item	Data Plan for the F01S300 Cabinet
EMU	Type: POWER4830L SN: 0 Subnode ID: 0 The subnode ID must be the same as the subnode setting of the corresponding DIP switches on the EMU, but the subnode ID must be different from IDs of the other subnodes on the same bus.
Charging parameters of the battery	Charging mode of the battery: automatic Equalized charging voltage of the battery: 56.5 V Float charging voltage of the battery: 53.5 V
Battery management parameters	Current-limiting coefficient for battery charging: 0.15 Interval of battery equalized charging: 60 days Number of battery sets: 1 Capacity of the battery set: 92 AH The battery capacity is configured according to the actual value. the F01S300 cabinet uses the 50 AH or 92 AH batteries.
The upper/lower temperature alarm limits or the upper/ lower temperature test limits	Upper temperature threshold of the battery set: 80°C Lower temperature threshold of the battery set: -20°C Temperature compensation coefficient of the battery set: 80 mV
Battery set power-off parameters	Battery set power-off permission status: permit Battery set power-off voltage: 43 V
Power distribution parameters	AC overvoltage alarm threshold of the power supply: 280 V AC undervoltage alarm threshold of the power supply: 180 V DC overvoltage alarm threshold of the power supply: 58 V DC undervoltage alarm threshold of the power supply: 45 V
Battery discharging test parameters	Battery auto-discharging test: auto-test Battery set auto-discharging test permission status: permit Battery auto-discharging test period: 60d
Power rectifier module parameters	The number of the power rectifier modules: 0 The number of the power rectifier modules is configured according to the actual value. EPS30-4815AF supports up to 2 rectifier modules.
Battery high-temperature power-off parameters	Battery high-temperature power-off permission status: permit Temperature for battery high-temperature power-off: 53°C

Copyright © Huawei Technologies Co., Ltd.

Item	Data Plan for the F01S300 Cabinet
Environment monitoring parameters	Upper alarm threshold of the temperature: 68°C Lower alarm threshold of the temperature: -5°C Upper test threshold of the humidity: 80°C Lower test threshold of the humidity: -20°C
External extended digital parameters	Digital parameter ID: 0 This digital parameter is set according to the actual requirements. The monitoring digital parameter of the external fan tray is set here to monitor the fan tray. When the fan tray is faulty, the host reports an alarm. Valid level of digital parameter 0: low level When the low level represents the valid level, the host does not report an alarm in the case of low level.
	Digital parameter ID: 1 This digital parameter is set according to the actual requirements. The monitoring digital parameter of the external fan tray is set here to monitor the fan tray. When the fan tray is faulty, the host reports an alarm. Valid level of digital parameter 1: low level When the low level represents the valid level, the host does not report an alarm in the case of low level.
	Digital parameter ID: 2 This digital parameter is set according to the actual requirements. Valid level of digital parameter 2: low level When the low level represents the valid level, the host does not report an alarm in the case of low level.
	Digital parameter ID: 3 This digital parameter is set according to the actual requirements. The monitoring digital parameter of the surge protector is set here to monitor the status of the surge protector. When the surge protector is faulty, the host reports an alarm. Valid level of digital parameter 3: low level When the low level represents the valid level, the host does not report an alarm in the case of low level.

Copyright © Huawei Technologies Co., Ltd.

Item	Data Plan for the F01S300 Cabinet
	Digital parameter ID: 4 This digital parameter is set according to the actual requirements. The monitoring digital parameter of the smoke sensor is set here to monitor whether there is smoke in the actual environment. When there is smoke, the host reports an alarm. Valid level of digital parameter 4: high level When the high level represents the valid level, the host does not report an alarm in the case of high level.
	Digital parameter ID: 5 This digital parameter is set according to the actual requirements. The monitoring digital parameter of the heat exchanger is set here to monitor the status of the heat exchanger. When the heat exchanger is faulty, the host reports an alarm. Valid level of digital parameter 5: low level When the low level represents the valid level, the host does not report an alarm in the case of low level.
	Digital parameter ID: 6 This digital parameter is set according to the actual requirements. The digital monitoring parameter of the MDF door status sensor is set here to monitor the MDF door status. When the door of the MDF compartment is open, the host reports an alarm. Valid level of digital parameter 6: low level When the low level represents the valid level, the host does not report an alarm in the case of low level.

NOTE

The preceding data is configured according to the actual requirements. When the actually planned value of a parameter is the same as the default value, it is not necessary to configure the parameter.

Configuration Example

The following considers the configuration in the F01S300 cabinet as an example to describe the process of configuring the environment monitoring parameters of the EPS30-4815AF.

```
huawei(config)#emu add 0 POWER4830L 0 0 POWER4830L
huawei(config)#display emu 0
huawei(config)#interface emu 0
huawei(config-if-power4830l-0)#display power system parameter
huawei(config-if-power4830l-0)#display power environment parameter
huawei(config-if-power4830l-0)#power battery parameter 1 0.15 60 92
huawei(config-if-power4830l-0)#power battery-test auto-test permit 60
huawei(config-if-power4830l-0)#power temperature-off battery-off-state permit
battery-off-temperature 53
huawei(config-if-power4830l-0)#power environment temperature 68 -5 80 -20
huawei(config-if-power4830l-0)#power outside-digital 3 available-level low-level
name SPD digital-alarm 20
huawei(config-if-power4830l-0)#power outside-digital 4 available-level high-level
```


Copyright © Huawei Technologies Co., Ltd.

```
name Smoke digital-alarm 15
huawei(config-if-power4830l-0)#power outside-digital 5 available-level low-level
name HEX digital-alarm 13
huawei(config-if-power4830l-0)#power outside-digital 6 available-level low-level
name MDF-door digital-alarm 9
huawei(config-if-power4830l-0)#display power system parameter
huawei(config-if-power4830l-0)#display power environment parameter
huawei(config-if-power4830l-0)#display power alarm
huawei(config-if-power4830l-0)#quit
huawei(config)#save
```

1.3.16.5 Configuring the Environment Monitoring Parameters of the EPS75-4815AF

This topic describes how to configure the environment monitoring parameters of the EPS75-4815AF through the CLI.

Mapping Between Monitoring Parameters and Device Ports

Table 1-28 describes the mapping between the monitoring parameters displayed on the sensor transfer box.

Table 1-28 Mapping between the monitoring parameters displayed on the host and the ports on the sensor transfer box

Monitoring Parameter Displayed on the Host	Device Port	Application in the N66 Cabinet	Application in the F01D500 Cabinet
Digital 0	JTD1	Not connected by default, used to add a user-defined monitoring digital parameter	Not connected by default, used to add a user-defined monitoring digital parameter
Digital 1	JTD2	Not connected by default, used to add a user-defined monitoring digital parameter	Not connected by default, used to add a user-defined monitoring digital parameter
Digital 2	JTD3	Not connected by default, used to add a user-defined monitoring digital parameter	Not connected by default, used to add a user-defined monitoring digital parameter
Digital 3	JTD4	Not connected by default, used to add a user-defined monitoring digital parameter	surge protector

Copyright © Huawei Technologies Co., Ltd.

Monitoring Parameter Displayed on the Host	Device Port	Application in the N66 Cabinet	Application in the F01D500 Cabinet
Digital 4	JTD5	Not connected by default, used to add a user-defined monitoring digital parameter	Smoke sensor
Digital 5	JTD6	Not connected by default, used to add a user-defined monitoring digital parameter	Heat exchanger
Digital 6	JTD7	Not connected by default, used to add a user-defined monitoring digital parameter	Door status sensor of the MDF compartment
Door alarm	JTM1	Not connected by default, used to monitor a door status sensor	Door status sensors of the device compartment and heat exchanger compartment
Wiring alarm	JTP1	Not connected by default, used to monitor a MDF sensor	MDF
Battery Tem	BAT_WE	Battery temperature sensor	Battery temperature sensor
environment Tem/environment Hum	TEM-HU	Not connected by default.	Temperature and humidity sensor

NOTE

Before adding a user-defined analog or monitoring digital parameter, make sure that the port corresponding to this parameter is properly connected to an environment monitoring cable.

Configuration Process

The monitoring parameters can be reported to the control system only when the data for the EPS75-4815AF is configured correctly in the system.

Table 1-29 lists the commands used during the configuration.

Copyright © Huawei Technologies Co., Ltd.

Table 1-29 Commands for configuring the EPS75-4815AF

To...	Run the Command...
Add an EMU	**emu add**
Query the configuration parameters of the power system	**display power system parameter**
Query the power environment parameters	**display power environment parameter**
Query the alarm information of the power supply	**display power alarm**
Configure the battery charging parameters	**power charge**
Configure the battery management parameters	**power battery parameter**
Configure the upper/lower temperature alarm limits or the upper/lower temperature test limits	**power battery temperature**
Configure the battery set power-off parameters	**power off**
Configure the power distribution parameters	**power supply-parameter**
Configure the battery discharging test parameters	**power battery-test**
Configure the parameters for the power rectifier module	**power module-num**
Configure the battery high-temperature power-off parameters	**power temperature-off**
Configure the environment monitoring parameters	**power environment**
Configure the external extended digital parameters	**power outside-digital**

1. Log in to the device through the maintenance terminal and add an EMU.
2. Query the status of the EPS75-4815AF.
3. Enter the environment monitoring configuration mode and query the default configuration.
4. Configure the battery management parameters.
5. Configure the battery discharging test parameters.

Copyright © Huawei Technologies Co., Ltd.

6. Configure the battery high-temperature power-off parameters.
7. Configure the environment parameters.
8. Configure the extended digital parameters.
9. Query the information about the configured parameters and environment parameters of the power system.
10. Query the alarms, and confirm that the door status alarm other than alarms for other monitoring parameters is generated. The door status sensors of the device compartment and the temperature control compartment are in serial connection, and are monitored as a variable.
11. Save the data.
12. Close all doors of the cabinet. Then, query the alarm information again, and confirm that there is no alarm for any monitoring parameter.

Data Plan

The data plan of the EPS75-4815AF in the N66 cabinet is the same as that in the F01D500 cabinets. In this topic, the application in the F01D500 cabinet is considered as an example. **Table 1-30** provides the data plan for configuring the monitoring parameters of the EPS75-4815AF.

Table 1-30 Data plan for configuring the monitoring parameters of the EPS75-4815AF

Item	Data Plan for the F01D500 Cabinet	Data Plan for the N66 Cabinet
EMU	Type: POWER4875L SN: 0 Subnode ID: 0 The subnode ID must be the same as the subnode setting of the corresponding DIP switches on the EMU, but the subnode ID must be different from IDs of the other subnodes on the same bus.	Type: POWER4875L SN: 0 Subnode ID: 0 The subnode ID must be the same as the subnode setting of the corresponding DIP switches on the EMU, but the subnode ID must be different from IDs of the other subnodes on the same bus.
Charging parameters of the battery	Charging mode of the battery: automatic Equalized charging voltage of the battery: 56.5 V Float charging voltage of the battery: 53.5 V	Charging mode of the battery: automatic Equalized charging voltage of the battery: 56.5 V Float charging voltage of the battery: 53.5 V

Copyright © Huawei Technologies Co., Ltd.

Item	Data Plan for the F01D500 Cabinet	Data Plan for the N66 Cabinet
Battery management parameters	Current-limiting coefficient for battery charging: 0.15 Interval of battery equalized charging: 60 days Number of battery sets: 1 Capacity of the battery set: 150 AH The battery capacity is configured according to the actual value. the F01D500 cabinet uses the 2 * 75 AH or 2 * 92 AH batteries.	Current-limiting coefficient for battery charging: 0.15 Interval of battery equalized charging: 60 days Number of battery sets: 1 The battery capacity is configured according to the actual value.
The upper/ lower temperature alarm limits or the upper/ lower temperature test limits	Upper temperature threshold of the battery set: 80°C Lower temperature threshold of the battery set: -20°C Temperature compensation coefficient of the battery set: 80 mV	Upper temperature threshold of the battery set: 80°C Lower temperature threshold of the battery set: -20°C Temperature compensation coefficient of the battery set: 80 mV
Battery set power-off parameters	Battery set power-off permission status: permit Battery set power-off voltage: 43 V	Battery set power-off permission status: permit Battery set power-off voltage: 43 V
Power distribution parameters	AC overvoltage alarm threshold of the power supply: 280 V AC undervoltage alarm threshold of the power supply: 180 V DC overvoltage alarm threshold of the power supply: 58 V DC undervoltage alarm threshold of the power supply: 45 V	AC overvoltage alarm threshold of the power supply: 280 V AC undervoltage alarm threshold of the power supply: 180 V DC overvoltage alarm threshold of the power supply: 58 V DC undervoltage alarm threshold of the power supply: 45 V
Battery discharging test parameters	Battery auto-discharging test: auto-test Battery set auto-discharging test permission status: permit Battery auto-discharging test period: 60d	Battery auto-discharging test: auto-test Battery set auto-discharging test permission status: permit Battery auto-discharging test period: 60d
Power rectifier module parameters	The number of the power rectifier modules: 0 The number of the power rectifier modules is configured according to the actual value. EPS75-4815AF supports up to 5 rectifier modules.	The number of the power rectifier modules: 0 The number of the power rectifier modules is configured according to the actual value. EPS75-4815AF supports up to 5 rectifier modules.

Copyright © Huawei Technologies Co., Ltd.

Item	Data Plan for the F01D500 Cabinet	Data Plan for the N66 Cabinet
Battery high-temperature power-off parameters	Battery high-temperature power-off permission status: permit Temperature for battery high-temperature power-off: 53°C	Battery high-temperature power-off permission status: permit Temperature for battery high-temperature power-off: 53°C
Environment monitoring parameters	Upper alarm threshold of the temperature: 68°C Lower alarm threshold of the temperature: -5°C Upper test threshold of the humidity: 80°C Lower test threshold of the humidity: -20°C	Upper alarm threshold of the temperature: 68°C Lower alarm threshold of the temperature: -5°C Upper test threshold of the humidity: 80°C Lower test threshold of the humidity: -20°C
External extended digital parameters	Digital parameter ID: 0 This digital parameter is set according to the actual requirements. The monitoring digital parameter of the external fan tray is set here to monitor the fan tray. When the fan tray is faulty, the host reports an alarm. Valid level of digital parameter 0: low level When the low level represents the valid level, the host does not report an alarm in the case of low level.	Digital parameter ID: 0 This digital parameter is set according to the actual requirements. The monitoring digital parameter of the external fan tray is set here to monitor the fan tray. When the fan tray is faulty, the host reports an alarm. Valid level of digital parameter 0: low level When the low level represents the valid level, the host does not report an alarm in the case of low level.
	Digital parameter ID: 1 This digital parameter is set according to the actual requirements. The monitoring digital parameter of the external fan tray is set here to monitor the fan tray. When the fan tray is faulty, the host reports an alarm. Valid level of digital parameter 1: low level When the low level represents the valid level, the host does not report an alarm in the case of low level.	Digital parameter ID: 1 This digital parameter is set according to the actual requirements. The monitoring digital parameter of the external fan tray is set here to monitor the fan tray. When the fan tray is faulty, the host reports an alarm. Valid level of digital parameter 1: low level When the low level represents the valid level, the host does not report an alarm in the case of low level.

Copyright © Huawei Technologies Co., Ltd.

Item	Data Plan for the F01D500 Cabinet	Data Plan for the N66 Cabinet
	Digital parameter ID: 2 This digital parameter is set according to the actual requirements. Valid level of digital parameter 2: low level When the low level represents the valid level, the host does not report an alarm in the case of low level.	Digital parameter ID: 2 This digital parameter is set according to the actual requirements. Valid level of digital parameter 2: low level When the low level represents the valid level, the host does not report an alarm in the case of low level.
	Digital parameter ID: 3 This digital parameter is set according to the actual requirements. The monitoring digital parameter of the surge protector is set here to monitor the status of the surge protector. When the surge protector is faulty, the host reports an alarm. Valid level of digital parameter 3: low level When the low level represents the valid level, the host does not report an alarm in the case of low level.	Digital parameter ID: 3 This digital parameter is set according to the actual requirements. The monitoring digital parameter of the surge protector is set here to monitor the status of the surge protector. When the surge protector is faulty, the host reports an alarm. Valid level of digital parameter 3: low level When the low level represents the valid level, the host does not report an alarm in the case of low level.
	Digital parameter ID: 4 This digital parameter is set according to the actual requirements. The monitoring digital parameter of the smoke sensor is set here to monitor whether there is smoke in the actual environment. When there is smoke, the host reports an alarm. Valid level of digital parameter 4: high level When the high level represents the valid level, the host does not report an alarm in the case of high level.	Digital parameter ID: 4 This digital parameter is set according to the actual requirements. The monitoring digital parameter of the smoke sensor is set here to monitor whether there is smoke in the actual environment. When there is smoke, the host reports an alarm. Valid level of digital parameter 4: high level When the high level represents the valid level, the host does not report an alarm in the case of high level.

Copyright © Huawei Technologies Co., Ltd.

Item	Data Plan for the F01D500 Cabinet	Data Plan for the N66 Cabinet
	Digital parameter ID: 5 This digital parameter is set according to the actual requirements. The monitoring digital parameter of the heat exchanger is set here to monitor the status of the heat exchanger. When the heat exchanger is faulty, the host reports an alarm. Valid level of digital parameter 5: low level When the low level represents the valid level, the host does not report an alarm in the case of low level.	Digital parameter ID: 5 This digital parameter is set according to the actual requirements. The monitoring digital parameter of the heat exchanger is set here to monitor the status of the heat exchanger. When the heat exchanger is faulty, the host reports an alarm. Valid level of digital parameter 5: low level When the low level represents the valid level, the host does not report an alarm in the case of low level.
	Digital parameter ID: 6 This digital parameter is set according to the actual requirements. The digital monitoring parameter of the MDF door status sensor is set here to monitor the MDF door status. When the door of the MDF compartment is open, the host reports an alarm. Valid level of digital parameter 6: low level When the low level represents the valid level, the host does not report an alarm in the case of low level.	Digital parameter ID: 6 This digital parameter is set according to the actual requirements. The digital monitoring parameter of the MDF door status sensor is set here to monitor the MDF door status. When the door of the MDF compartment is open, the host reports an alarm. Valid level of digital parameter 6: low level When the low level represents the valid level, the host does not report an alarm in the case of low level.

NOTE

The preceding data is configured according to the actual requirements. When the actually planned value of a parameter is the same as the default value, it is not necessary to configure the parameter.

Configuration Example

The following considers the configuration in the F01D500 cabinet as an example to describe the process of configuring the environment monitoring parameters of the EPS75-4815AF.

```
huawei(config)#emu add 0 POWER4875L 0 0 POWER4875L
huawei(config)#display emu 0
huawei(config)#interface emu 0
huawei(config-if-power4875l-0)#display power system parameter
huawei(config-if-power4875l-0)#display power environment parameter
huawei(config-if-power4875l-0)#power battery parameter 1 0.15 60 150
huawei(config-if-power4875l-0)#power battery-test auto-test permit 60
```


Copyright © Huawei Technologies Co., Ltd.

```
huawei(config-if-power4875l-0)#power temperature-off battery-off-state permit
battery-off-temperature 53
huawei(config-if-power4875l-0)#power environment temperature 68 -5 80 -20
huawei(config-if-power4875l-0)#power outside-digital 3 available-level low-level
name SPD digital-alarm 20
huawei(config-if-power4875l-0)#power outside-digital 4 available-level high-level
name Smoke digital-alarm 15
huawei(config-if-power4875l-0)#power outside-digital 5 available-level low-level
name HEX digital-alarm 13
huawei(config-if-power4875l-0)#power outside-digital 6 available-level low-level
name MDF-door digital-alarm 9
huawei(config-if-power4875l-0)#display power system parameter
huawei(config-if-power4875l-0)#display power environment parameter
huawei(config-if-power4875l-0)#display power alarm
huawei(config-if-power4875l-0)#quit
huawei(config)#save
```

1.3.16.6 Configuring the Environment Monitoring Parameters of the GEPS4845

This topic describes how to configure the environment monitoring parameters of the GEPS4845 through the CLI.

Mapping Between Monitoring Parameters and Device Ports

Table 1-31 describes the mapping between the monitoring parameters displayed on the sensor transfer box.

Table 1-31 Mapping between the monitoring parameters displayed on the host and the ports on the sensor transfer box

Monitoring Parameter Displayed on the Host	Device Port	Application in the F01D500 Cabinet
Digital 0	JTD1	Not connected by default, used to add a user-defined monitoring digital parameter
Digital 1	JTD2	Not connected by default, used to add a user-defined monitoring digital parameter
Digital 2	JTD3	Not connected by default, used to add a user-defined monitoring digital parameter
Digital 3	JTD4	surge protector (SPD)
Digital 4	JTD5	Smoke sensor
Digital 5	JTD6	Heat exchanger
Digital 6	JTD7	Door status sensor of the MDF compartment
Door alarm	JTM1	Door status sensors of the device compartment and heat exchanger compartment

Copyright © Huawei Technologies Co., Ltd.

Monitoring Parameter Displayed on the Host	Device Port	Application in the F01D500 Cabinet
Wiring alarm	JTP1	MDF
Battery Tem	BAT_WE	Battery temperature sensor
environment Tem/ environment Hum	TEM-HU	Temperature and humidity sensor

NOTE

Before adding a user-defined analog or monitoring digital parameter, make sure that the port corresponding to this parameter is properly connected to an environment monitoring cable.

Configuration Process

The monitoring parameters can be reported to the control system only when the data for the GEPS4845 is configured correctly in the system.

Table 1-32 lists the commands used during the configuration.

Table 1-32 Commands for configuring the GEPS4845

To...	Run the Command...
Add an EMU	**emu add**
Query the configuration parameters of the power system	**display power system parameter**
Query the power environment parameters	**display power environment parameter**
Query the alarm information of the power supply	**display power alarm**
Configure the battery charging parameters	**power charge**
Configure the battery management parameters	**power battery parameter**
Configure the upper/lower temperature alarm limits or the upper/lower temperature test limits	**power battery temperature**
Configure the power supply load power-off and battery set power-off parameters	**power off**

Copyright © Huawei Technologies Co., Ltd.

To...	Run the Command...
Configure the power distribution parameters	**power supply-parameter**
Configure the battery discharging test parameters	**power battery-test**
Configure the parameters for the power rectifier module	**power module-num**
Configure the environment monitoring parameters	**power environment**
Configure the load and battery high-temperature power-off parameters	**power temperature-off**
Configure the external extended digital parameters	**power outside-digital**

1. Log in to the device through the maintenance terminal and add an EMU.
2. Query the status of the GEPS4845.
3. Enter the environment monitoring configuration mode and query the default configuration.
4. Configure the battery management parameters.
5. Configure the battery discharging test parameters.
6. Configure the environment parameters.
7. Configure the load and battery high-temperature power-off parameters.
8. Configure the extended digital parameters.
9. Query the information about the configured parameters and environment parameters of the power system.
10. Query the alarms, and confirm that the door status alarm other than alarms for other monitoring parameters is generated. The door status sensors of the device compartment and the temperature control compartment are in serial connection, and are monitored as a variable.
11. Save the data.
12. Close all doors of the cabinet. Then, query the alarm information again, and confirm that there is no alarm for any monitoring parameter.

Data Plan

In this topic, the application in the F01D500 cabinet is considered as an example. **Table 1-33** provides the data plan for configuring the monitoring parameters of the GEPS4845.

Copyright © Huawei Technologies Co., Ltd.

Table 1-33 Data plan for configuring the monitoring parameters of the GEPS4845

Item	Data Plan for the F01D500 Cabinet
EMU	Type: POWER4845 SN: 0 Subnode ID: 0 The subnode ID must be the same as the subnode setting of the corresponding DIP switches on the EMU, but the subnode ID must be different from IDs of the other subnodes on the same bus.
Charging parameters of the battery	Charging mode of the battery: automatic Equalized charging voltage of the battery: 56.5 V Float charging voltage of the battery: 53.5 V
Battery management parameters	Current-limiting coefficient for battery charging: 0.15 Interval of battery equalized charging: 60 days Number of battery sets: 1 Capacity of the battery set: 150 AH The battery capacity is configured according to the actual value. the F01D500 cabinet uses the 2 * 75 AH or 2 * 92 AH batteries.
The upper/lower temperature alarm limits or the upper/lower temperature test limits	Upper temperature threshold of the battery set: 60°C Lower temperature threshold of the battery set: -40°C Temperature compensation coefficient of the battery set: 100 mV
Power supply load power-off and battery set power-off parameters	Load power-off permission status: forbid Battery set power-off permission status: permit Load power-off voltage: 44 V Battery set power-off voltage: 43 V
Power distribution parameters	AC overvoltage alarm threshold of the power supply: 280 V AC undervoltage alarm threshold of the power supply: 180 V DC overvoltage alarm threshold of the power supply: 58 V DC undervoltage alarm threshold of the power supply: 45 V
Battery discharging test parameters	Battery auto-discharging test: auto-test Battery set auto-discharging test permission status: permit Battery auto-discharging test period: 60d
Power rectifier module parameters	The number of the power rectifier modules: 0 The number of the power rectifier modules is configured according to the actual value. GEPS4845 supports up to 3 rectifier modules.

Copyright © Huawei Technologies Co., Ltd.

Item	Data Plan for the F01D500 Cabinet
Environment monitoring parameters	Upper alarm threshold of the temperature: 68°C Lower alarm threshold of the temperature: -5°C Upper test threshold of the humidity: 80°C Lower test threshold of the humidity: -20°C
Load and battery high-temperature power-off parameters	Load high-temperature power-off permission status: forbid Battery high-temperature power-off permission status: permit Temperature for load high-temperature power-off: 70°C Temperature for battery high-temperature power-off: 53°C
External extended digital parameters	Digital parameter ID: 0 This digital parameter is set according to the actual requirements. The monitoring digital parameter of the external fan tray is set here to monitor the fan tray. When the fan tray is faulty, the host reports an alarm. Valid level of digital parameter 0: low level When the low level represents the valid level, the host does not report an alarm in the case of low level.
	Digital parameter ID: 1 This digital parameter is set according to the actual requirements. The monitoring digital parameter of the external fan tray is set here to monitor the fan tray. When the fan tray is faulty, the host reports an alarm. Valid level of digital parameter 1: low level When the low level represents the valid level, the host does not report an alarm in the case of low level.
	Digital parameter ID: 2 This digital parameter is set according to the actual requirements. Valid level of digital parameter 2: low level When the low level represents the valid level, the host does not report an alarm in the case of low level.
	Digital parameter ID: 3 This digital parameter is set according to the actual requirements. The monitoring digital parameter of the surge protector is set here to monitor the status of the surge protector. When the surge protector is faulty, the host reports an alarm. Valid level of digital parameter 3: low level When the low level represents the valid level, the host does not report an alarm in the case of low level.

Copyright © Huawei Technologies Co., Ltd.

Item	Data Plan for the F01D500 Cabinet
	Digital parameter ID: 4 This digital parameter is set according to the actual requirements. The monitoring digital parameter of the smoke sensor is set here to monitor whether there is smoke in the actual environment. When there is smoke, the host reports an alarm. Valid level of digital parameter 4: high level When the high level represents the valid level, the host does not report an alarm in the case of high level.
	Digital parameter ID: 5 This digital parameter is set according to the actual requirements. The monitoring digital parameter of the heat exchanger is set here to monitor the status of the heat exchanger. When the heat exchanger is faulty, the host reports an alarm. Valid level of digital parameter 5: low level When the low level represents the valid level, the host does not report an alarm in the case of low level.
	Digital parameter ID: 6 This digital parameter is set according to the actual requirements. The digital monitoring parameter of the MDF door status sensor is set here to monitor the MDF door status. When the door of the MDF compartment is open, the host reports an alarm. Valid level of digital parameter 6: low level When the low level represents the valid level, the host does not report an alarm in the case of low level.

NOTE

The preceding data is configured according to the actual requirements. When the actually planned value of a parameter is the same as the default value, it is not necessary to configure the parameter.

Configuration Example

The following considers the configuration in the F01D500 cabinet as an example to describe the process of configuring the environment monitoring parameters of the GEPS4845.

```
huawei(config)#emu add 0 POWER4845 0 0 POWER4845
huawei(config)#display emu 0
huawei(config)#interface emu 0
huawei(config-if-power4845-0)#display power system parameter
huawei(config-if-power4845-0)#display power environment parameter
huawei(config-if-power4845-0)#power battery parameter 1 0.15 60 150
huawei(config-if-power4845-0)#power battery-test auto-test permit 60
huawei(config-if-power4845-0)#power environment temperature 68 -5 80 -20
huawei(config-if-power4845-0)#power temperature-off load-off-state forbid load-
off-temperature 70 battery-off-state permit battery-off-temperature 53
huawei(config-if-power4845-0)#power outside-digital 3 available-level low-level
name SPD digital-alarm 20
huawei(config-if-power4845-0)#power outside-digital 4 available-level high-level
```


Copyright © Huawei Technologies Co., Ltd.

```
name Smoke digital-alarm 15
huawei(config-if-power4845-0)#power outside-digital 5 available-level low-level
name HEX digital-alarm 13
huawei(config-if-power4845-0)#power outside-digital 6 available-level low-level
name MDF-door digital-alarm 9
huawei(config-if-power4845-0)#display power system parameter
huawei(config-if-power4845-0)#display power environment parameter
huawei(config-if-power4845-0)#display power alarm
huawei(config-if-power4845-0)#quit
huawei(config)#save
```

1.3.16.7 Configuring the Environment Monitoring Parameters of the ETP4830

This topic describes how to configure the environment monitoring parameters of the ETP4830 through the CLI.

Mapping Between Monitoring Parameters and Device Ports

The ETP4830 monitoring scheme can be used in the F01S300 cabinet. **Table 1-34** describes the mapping between the monitoring parameters displayed

NOTE

Before adding a user-defined analog or monitoring digital parameter, make sure that the port corresponding to this parameter is properly connected to an environment monitoring cable.

Table 1-34 Mapping between the monitoring parameters displayed on the host and the ports on the sensor transfer box

Monitoring Parameter Displayed on the Host	Device Port	Application in the F01S300 Cabinet
Digital 0	JTD1	Not connected by default, used to add a user-defined monitoring digital parameter
Digital 1	JTD2	Battery compartment heater (optional configuration)
Digital 2	JTD3	Device compartment heater (optional configuration)
Digital 3	JTD4	Surge protector
Digital 4	JTD5	Not connected by default, used to add a user-defined monitoring digital parameter
Digital 5	JTD6	Heat exchanger
Digital 6	JTD7	Door status sensor of the MDF compartment
Door alarm	JTM1	Door status sensors of the device compartment and heat exchanger compartment
Wiring alarm	JTP1	MDF
Battery Tem	VBTEM2	Battery temperature sensor

Copyright © Huawei Technologies Co., Ltd.

Monitoring Parameter Displayed on the Host	Device Port	Application in the F01S300 Cabinet
Environment Tem	VTEM2	Environment temperature sensor
Smoke	SMOKE	Smoke sensor (optional configuration)
Water	WATER	Water sensor (optional configuration)

Procedure

Step 1 Log in to the device through the maintenance terminal and add an ETP4830 (SMU).

Run the **emu add** command to add the SMU.

Step 2 Check the default configurations of the power system.

Run the **interface emu** command to enter environment monitoring mode and then run the **display power system parameter** and **display power environment parameter** commands to query the default configurations.

Step 3 Configure parameters required for lead-acid batteries.

Run the **power battery parameter** command to configure parameters required for batteries, including the management parameters, charging parameters, power-off parameters, and high-temperature power-off parameters. You can use default values of these parameters for configuration.

Step 4 Run the **power battery temperature** command to configure the upper/lower temperature test limits, temperature compensation coefficient, and the upper/lower alarm temperature limits of the battery set.

Step 5 (Optional) Configure discharging testing parameters.

- Run the **power battery-test** command to configure the discharging testing parameters, including the automatic power-off test, scheduled automatic test, test interval for automatic discharging, test time for delayed discharging, voltage at the stop of the test, number of batteries in a battery set, time limit for the discharging test, time limit for simplified discharging test, alarm thresholds for discharging efficiencies. You can use default values of these parameters for configuration.
- Run the **display power battery-test info** command to query the discharge testing information about the batteries.

Step 6 Run the **power off** command to configure the load power-off and battery set power-off voltage parameters

Step 7 Run the **power temperature-off** command to configure the battery high-temperature power-off parameters.

Step 8 Configure the environment monitoring parameters of the SMU system.

Run the **power environment** command to configure the upper alarm threshold and the upper and lower test thresholds for the temperatures and humidity. After these parameters are set, the

Copyright © Huawei Technologies Co., Ltd.

system reports alarms if the working environment of the power system does not meet requirements.

Step 9 Configure required parameters for the rectifier module.

Run the **power module-num** command to configure the required parameters for the rectifier module.

Step 10 Configure the external extended digital variables of the power system.

Run the **power outside-digital** command to configure the external extended digital variables of the power system.

Step 11 Query the information about the configuration parameters and environment parameters of the power system.

Run the **display power system parameter** and **display power environment parameter** commands to query the configuration parameters and environment parameters of the power system.

Step 12 Run the **display power alarm** command to query the alarm information, and ensure that no alarm is generated for the monitored objects except the door status.

Step 13 Save the data.

Run the **quit** command to exit the SMU mode, and run the **save** command to save the data.

----End

Result

After the configuration, the ETP4830 power system works properly and monitors the configured parameters. If the status of a monitored parameter becomes abnormal, an alarm is generated on the device.

Data Plan

Table 1-35 provides the data plan for configuring the monitoring parameters of the ETP4830.

Table 1-35 Data plan for configuring the power monitoring using the ETP4830

Item	Data Plan for the F01S300 Cabinet
EMU	Type: SMU SN: 1 Subnode ID: 0 **NOTE** The subnode ID must be the same as the subnode setting of the corresponding DIP switches on the EMU, but the subnode ID must be different from IDs of the other subnodes on the same bus.
Charging parameters of the battery	Charging mode of the battery: automatic Equalized charging voltage of the battery (V): 56.5 Float charging voltage of the battery (V): 53.5

Copyright © Huawei Technologies Co., Ltd.

Item	Data Plan for the F01S300 Cabinet
Battery management parameters	Current-limiting coefficient for battery charging: ● One 50 AH battery set: 0.15 ● One 92 AH battery set: 0.1 Interval of battery equalized charging (day): 60 Number of battery sets: 1 Capacity of the battery set: ● One 50 AH battery set: 50 ● One 92 AH battery set: 92
The upper/lower temperature test limits or temperature compensation coefficient of the battery set	Upper temperature threshold of the battery set (°C): 80 Lower temperature threshold of the battery set (°C): -20 Temperature compensation coefficient of the battery set (mV): 80
The upper/lower temperature alarm limits of the battery set	Upper temperature alarm limit of the battery set (°C): 50 Lower temperature alarm limit of the battery set (°C): -15
Battery discharging test parameters	Battery auto-discharging test: auto-test Battery set auto-discharging test permission status: permit Battery auto-discharging test period (day): 120
Load power-off and battery set power-off voltage parameters	Battery set power-off permission status: permit Battery set power-off voltage (V): 43
Battery high-temperature power-off parameters	Battery high-temperature power-off permission status: permit Temperature for battery high-temperature power-off (°C): 53
Environment temperature parameters	Upper alarm threshold of the temperature (°C): 68 Lower alarm threshold of the temperature (°C): -20 Upper test threshold of the temperature (°C): 80 Lower test threshold of the temperature (°C): -20
Environment humidity parameters	Upper alarm threshold of the humidity (% RH): 80 Lower alarm threshold of the humidity (% RH): 0 Upper test threshold of the humidity (% RH): 100 Lower test threshold of the humidity (% RH): 0
Power rectifier module parameters	The number of the power rectifier modules is configured according to the actual value. ETP4830 supports up to 2 rectifier modules.

Copyright © Huawei Technologies Co., Ltd.

Item	Data Plan for the F01S300 Cabinet
External extended digital parameters	Digital parameter ID: 2 Available-level: low level Name: Batt-heater **NOTE** The monitoring digital parameter of the battery compartment heater (optional configuration) is set here to monitor the battery compartment heater. When the battery compartment heater is faulty, the device reports an alarm. The battery compartment heater has the low level when working properly and the device does not report an alarm.
	Digital parameter ID: 3 Available-level: low level Name: Eqiup-heater **NOTE** The monitoring digital parameter of the equipment compartment heater (optional configuration) is set here to monitor the equipment compartment heater. When the equipment compartment heater is faulty, the device reports an alarm. The equipment compartment heater has the low level when working properly and the device does not report an alarm.
	Digital parameter ID: 4 Available-level: low level Name: SPD Digital-alarm-index: 20 **NOTE** The monitoring digital parameter of the surge protector is set here to monitor the surge protector. When the surge protector is faulty, the device reports an alarm. The surge protector has the low level when working properly and the device does not report an alarm.
	Digital parameter ID: 6 Available-level: low level Name: HEX Digital-alarm-index: 13 **NOTE** The monitoring digital parameter of the heat exchanger is set here to monitor the status of the heat exchanger. When the heat exchanger is faulty, the device reports an alarm. The heat exchanger has the low level when working properly and the device does not report an alarm.

Copyright © Huawei Technologies Co., Ltd.

Item	Data Plan for the F01S300 Cabinet
	Digital parameter ID: 7 Available-level: low level Name: MDF-door Digital-alarm-index: 9 **NOTE** The digital monitoring parameter of the MDF door status sensor is set here to monitor the MDF door status. When the door of the MDF compartment is open, the device reports an alarm. The MDF compartment has the low level when its door is closed and the device does not report an alarm.

NOTE

The preceding data is configured according to the actual requirements. When the actually planned value of a parameter is the same as the default value, it is not necessary to configure the parameter.

Example

Assume that the F01S300 cabinet is configured with one 50 AH battery set, the ETP4830 is configured with 2 rectifier modules, and battery compartment heater and equipment compartment heater are configured. To configure the environment monitoring parameters of the ETP4830, do as follows:

```
huawei(config)#emu add 1 SMU 0 0 SMU
huawei(config)#display emu 1
huawei(config)#interface emu 1
huawei(config-if-smu-1)#display power system parameter
huawei(config-if-smu-1)#display power environment parameter
huawei(config-if-smu-1)#power battery parameter 1 0.15 60 50
huawei(config-if-smu-1)#power battery temperature 80 -20 80
huawei(config-if-smu-1)#power battery temperature alarm_upper-limit 50 alarm_lower-
limit -15
huawei(config-if-smu-1)#power battery-test auto-test permit 120
huawei(config-if-smu-1)#display power battery-test info 1
huawei(config-if-smu-1)#power off battery-off-state permit battery-off-voltage 43
huawei(config-if-smu-1)#power temperature-off battery-off-state permit battery-off-
temperature 53
huawei(config-if-smu-1)#power environment temperature 68 -20 80 -20
  This command is invalid unless in the contition of install the sensor, would
you continue? (y/n)[n]:y
huawei(config-if-smu-1)#power environment humidity 80 0 100 0
  This command is invalid unless in the contition of install the sensor, would
you continue? (y/n)[n]:y
huawei(config-if-smu-1)#power module-num 2 1 2
huawei(config-if-smu-1)#power outside-digital 2 available-level low-level name
Batt-heater
huawei(config-if-smu-1)#power outside-digital 3 available-level low-level name
Equip-heater
huawei(config-if-smu-1)#power outside-digital 4 available-level low-level name SPD
digital-alarm 20
huawei(config-if-smu-1)#power outside-digital 6 available-level low-level name HEX
digital-alarm 13
huawei(config-if-smu-1)#power outside-digital 7 available-level low-level name MDF-
door digital-alarm 9
huawei(config-if-smu-1)#display power system parameter
huawei(config-if-smu-1)#display power environment parameter
huawei(config-if-smu-1)#display power alarm
```


Copyright © Huawei Technologies Co., Ltd.

```
huawei(config-if-smu-1)#quit
huawei(config)#save
```

1.3.16.8 Configuring the Environment Monitoring Parameters of the ETP4890

This topic describes how to configure the environment monitoring parameters of the ETP4890 through the CLI.

Mapping Between Monitoring Parameters and Device Ports

The ETP4890 monitoring scheme can be used in the F01D500 cabinet. **Table 1-36** describes the mapping between the monitoring parameters displayed

NOTE

Before adding a user-defined analog or monitoring digital parameter, make sure that the port corresponding to this parameter is properly connected to an environment monitoring cable.

Table 1-36 Mapping between the monitoring parameters displayed on the host and the ports on the sensor transfer box

Monitoring Parameter Displayed on the Host	Device Port	Application in the F01S300 Cabinet
Digital 0	JTD1	Not connected by default, used to add a user-defined monitoring digital parameter
Digital 1	JTD2	Not connected by default, used to add a user-defined monitoring digital parameter
Digital 2	JTD3	Not connected by default, used to add a user-defined monitoring digital parameter
Digital 3	JTD4	Surge protector (SPD)
Digital 4	JTD5	Not connected by default, used to add a user-defined monitoring digital parameter
Digital 5	JTD6	Heat exchanger
Digital 6	JTD7	Door status sensor of the MDF compartment
Door alarm	JTM1	Door status sensors of the device compartment and heat exchanger compartment
Wiring alarm	JTP1	MDF
Battery Tem	VBTEM2	Battery temperature sensor
environment Tem	VTEM2	Environment temperature sensor

Copyright © Huawei Technologies Co., Ltd.

Monitoring Parameter Displayed on the Host	Device Port	Application in the F01S300 Cabinet
Smoke	SMOKE	Smoke sensor

Procedure

Step 1 Log in to the device through the maintenance terminal and add an ETP4890 (SMU).

Run the **emu add** command to add the SMU.

Step 2 Check the default configurations of the power system.

Run the **interface emu** command to enter environment monitoring mode and then run the **display power system parameter** and **display power environment parameter** commands to query the default configurations.

Step 3 Configure parameters required for lead-acid batteries.

Run the **power battery parameter** command to configure parameters required for batteries, including the management parameters, charging parameters, power-off parameters, and high-temperature power-off parameters. You can use default values of these parameters for configuration.

Step 4 Run the **power battery temperature** command to configure the upper/lower temperature test limits, temperature compensation coefficient, and the upper/lower alarm temperature limits of the battery set.

Step 5 (Optional) Configure discharging testing parameters.

- Run the **power battery-test** command to configure the discharging testing parameters, including the automatic power-off test, scheduled automatic test, test interval for automatic discharging, test time for delayed discharging, voltage at the stop of the test, number of batteries in a battery set, time limit for the discharging test, time limit for simplified discharging test, alarm thresholds for discharging efficiencies. You can use default values of these parameters for configuration.
- Run the **display power battery-test info** command to query the discharge testing information about the batteries.

Step 6 Run the **power off** command to configure the load power-off and battery set power-off voltage parameters

Step 7 Run the **power temperature-off** command to configure the battery high-temperature power-off parameters.

Step 8 Configure the environment monitoring parameters of the SMU system.

Run the **power environment** command to configure the upper alarm threshold and the upper and lower test thresholds for the temperatures and humidity. After these parameters are set, the system reports alarms if the working environment of the power system does not meet requirements.

Step 9 Configure required parameters for the rectifier module.

Copyright © Huawei Technologies Co., Ltd.

Run the **power module-num** command to configure the required parameters for the rectifier module.

Step 10 Configure the external extended digital variables of the power system.

Run the **power outside-digital** command to configure the external extended digital variables of the power system.

Step 11 Query the information about the configuration parameters and environment parameters of the power system.

Run the **display power system parameter** and **display power environment parameter** commands to query the configuration parameters and environment parameters of the power system.

Step 12 Run the **display power alarm** command to query the alarm information, and ensure that no alarm is generated for the monitored objects except the door status.

Step 13 Save the data.

Run the **quit** command to exit the SMU mode, and run the **save** command to save the data.

----End

Result

After the configuration, the ETP4890 power system works properly and monitors the configured parameters. If the status of a monitored parameter becomes abnormal, an alarm is generated on the device.

Data Plan

Table 1-37 provides the data plan for configuring the monitoring parameters of the ETP4890.

Table 1-37 Data plan for configuring the power monitoring using the ETP4890

Item	Data Plan for the F01D500 Cabinet
EMU	Type: SMU SN: 0 Subnode ID: 0 **NOTE** The subnode ID must be the same as the subnode setting of the corresponding DIP switches on the EMU, but the subnode ID must be different from IDs of the other subnodes on the same bus.
Charging parameters of the battery	Charging mode of the battery: automatic Equalized charging voltage of the battery (V): 56.5 Float charging voltage of the battery (V): 53.5

Copyright © Huawei Technologies Co., Ltd.

Item	Data Plan for the F01D500 Cabinet
Battery management parameters	Current-limiting coefficient for battery charging: 0.15 Interval of battery equalized charging (day): 60 Number of battery sets: 1 Capacity of the battery set: ● Two 75 AH battery sets: 150 ● Two 92 AH battery sets: 184
The upper/lower temperature test limits or temperature compensation coefficient of the battery set	Upper temperature threshold of the battery set (°C): 80 Lower temperature threshold of the battery set (°C): -20 Temperature compensation coefficient of the battery set (mV): 80
The upper/lower temperature alarm limits of the battery set	Upper temperature alarm limit of the battery set (°C): 50 Lower temperature alarm limit of the battery set (°C): -15
Battery discharging test parameters	Battery auto-discharging test: auto-test Battery set auto-discharging test permission status: permit Battery auto-discharging test period (day): 180
Load power-off and battery set power-off voltage parameters	Load power-off status: forbid Load power-off voltage (V): 44 Battery set power-off permission status: permit Battery set power-off voltage (V): 43
Battery high-temperature power-off parameters	Battery high-temperature power-off permission status: permit Temperature for battery high-temperature power-off (°C): 53
Environment temperature parameters	Upper alarm threshold of the temperature (°C): 68 Lower alarm threshold of the temperature (°C): -5 Upper test threshold of the temperature (°C): 80 Lower test threshold of the temperature (°C): -20
Environment humidity parameters	Upper alarm threshold of the humidity (% RH): 80 Lower alarm threshold of the humidity (% RH): 0 Upper test threshold of the humidity (% RH): 100 Lower test threshold of the humidity (% RH): 0
Power rectifier module parameters	The number of the power rectifier modules is configured according to the actual value. ETP4890 supports up to 3 rectifier modules.

Copyright © Huawei Technologies Co., Ltd.

Item	Data Plan for the F01D500 Cabinet
External extended digital parameters	Digital parameter ID: 3 Available-level: low level Name: SPD Digital-alarm-index: 20 **NOTE** The monitoring digital parameter of the surge protector is set here to monitor the surge protector. When the surge protector is faulty, the device reports an alarm. The surge protector has the low level when working properly and the device does not report an alarm.
	Digital parameter ID: 5 Available-level: low level Name: HEX Digital-alarm-index: 13 **NOTE** The monitoring digital parameter of the heat exchanger is set here to monitor the status of the heat exchanger. When the heat exchanger is faulty, the device reports an alarm. The heat exchanger has the low level when working properly and the device does not report an alarm.
	Digital parameter ID: 6 Available-level: low level Name: MDF-door Digital-alarm-index: 9 **NOTE** The digital monitoring parameter of the MDF door status sensor is set here to monitor the MDF door status. When the door of the MDF compartment is open, the device reports an alarm. The MDF compartment has the low level when its door is closed and the device does not report an alarm.

NOTE

The preceding data is configured according to the actual requirements. When the actually planned value of a parameter is the same as the default value, it is not necessary to configure the parameter.

Example

Assume that the F01D500 cabinet is configured with two 75 AH battery sets, the ETP4890 is configured with 3 rectifier modules. To configure the environment monitoring parameters of the ETP4890, do as follows:

```
huawei(config)#emu add 1 SMU 0 0 ETP4890
huawei(config)#display emu 1
huawei(config)#interface emu 1
huawei(config-if-smu-1)#display power system parameter
huawei(config-if-smu-1)#display power environment parameter
huawei(config-if-smu-1)#power battery parameter 0.15 60 1 150
huawei(config-if-smu-1)#power battery temperature 80 -20 80
huawei(config-if-smu-1)#power battery temperature alarm_upper-limit 50 alarm_lower-
```


Copyright © Huawei Technologies Co., Ltd.

```
limit -15
huawei(config-if-smu-1)#power battery-test auto-test permit 180
huawei(config-if-smu-1)#display power battery-test info 1
huawei(config-if-smu-1)#power off load-off-state forbid load-off-voltage 44
battery-off-state permit battery-off-voltage 43
huawei(config-if-smu-1)#power temperature-off battery-off-state permit battery-off-
temperature 53
huawei(config-if-smu-1)#power environment temperature 68 -5 80 -20
  This command is invalid unless in the contition of install the sensor, would
you continue? (y/n)[n]:y
huawei(config-if-smu-1)#power environment humidity 80 0 100 0
  This command is invalid unless in the contition of install the sensor, would
you continue? (y/n)[n]:y
huawei(config-if-smu-1)#power module-num 3 1 2 3
huawei(config-if-smu-1)#power outside-digital 3 available-level low-level name SPD
digital-alarm 20
huawei(config-if-smu-1)#power outside-digital 5 available-level low-level name HEX
digital-alarm 13
huawei(config-if-smu-1)#power outside-digital 6 available-level low-level name MDF-
door digital-alarm 9
huawei(config-if-smu-1)#display power system parameter
huawei(config-if-smu-1)#display power environment parameter
huawei(config-if-smu-1)#display power alarm
huawei(config-if-smu-1)#quit
huawei(config)#save
```

1.3.16.9 Configuring the Power3000 Environment Monitoring Mode

This topic describes how to configure environment monitoring parameters by using the CLI.

Configuration Process

The monitoring parameters can be reported to the control system only when the data for the Power3000 is configured correctly in the system.

Table 1-38 lists the commands used during the configuration.

Table 1-38 Commands for configuring the Power3000

To...	Run the Command...
Add an EMU	**emu add**
Query the configuration parameters of the power system	**display power system parameter**
Query the power environment parameters	**display power environment parameter**
Configure the battery charging parameters	**power charge**
Configure the battery management parameters	**power battery parameter**
Configure the upper/lower temperature alarm limits or the upper/lower temperature test limits	**power battery temperature**

Copyright © Huawei Technologies Co., Ltd.

To...	Run the Command...
Configure the battery set power-off parameters	**power off**
Configure the power distribution parameters	**power supply-parameter**
Configure the battery discharging test parameters	**power battery-test**
Configure the parameters for the power rectifier module	**power module-num**
Configure the battery high-temperature power-off parameters	**power temperature-off**
Configure the environment monitoring parameters	**power environment**
Configure the external extended digital parameters	**power outside-digital**

1. Log in to the device through the maintenance terminal and add an EMU.
2. Query the status of the Power3000.
3. Enter the environment monitoring configuration mode and query the default configuration.
4. Configure the battery management parameters.
5. Configure the battery discharging test parameters.
6. Configure the battery high-temperature power-off parameters.
7. Configure the environment parameters.
8. Configure the extended digital parameters.
9. Query the information about the configured parameters and environment parameters of the power system.
10. Save the data.

Data Plan

Table 1-39 provides the data plan for configuring the monitoring parameters of the Power3000.

Copyright © Huawei Technologies Co., Ltd.

Table 1-39 Data plan for configuring the monitoring parameters of the Power3000

Item	Data Plan
EMU	Type: POWER3000 SN: 0 Subnode ID: 0 The subnode ID must be the same as the subnode setting of the corresponding DIP switches on the EMU, but the subnode ID must be different from IDs of the other subnodes on the same bus.
Charging parameters of the battery	Charging mode of the battery: automatic Equalized charging voltage of the battery: 56.5 V Float charging voltage of the battery: 53.5 V
Battery management parameters	Current-limiting coefficient for battery charging: 0.15 Interval of battery equalized charging: 60 days Number of battery sets: 1 Capacity of the battery set: 65 AH The battery capacity is configured according to the actual value.
The upper/lower temperature alarm limits or the upper/lower temperature test limits	Upper temperature threshold of the battery set: 80°C Lower temperature threshold of the battery set: -20°C Temperature compensation coefficient of the battery set: 80 mV
Battery set power-off parameters	Battery set power-off permission status: permit Battery set power-off voltage: 43 V
Power distribution parameters	AC overvoltage alarm threshold of the power supply: 280 V AC undervoltage alarm threshold of the power supply: 180 V DC overvoltage alarm threshold of the power supply: 58 V DC undervoltage alarm threshold of the power supply: 45 V
Battery discharging test parameters	Battery auto-discharging test: auto-test Battery set auto-discharging test permission status: permit Battery auto-discharging test period: 60d
Power rectifier module parameters	The number of the power rectifier modules: 0 The number of the power rectifier modules is configured according to the actual value. POWER3000 supports up to 12 rectifier modules.
Battery high-temperature power-off parameters	Battery high-temperature power-off permission status: permit Temperature for battery high-temperature power-off: 53°C

Copyright © Huawei Technologies Co., Ltd.

Item	Data Plan
Environment monitoring parameters	Upper alarm threshold of the temperature: 68°C Lower alarm threshold of the temperature: -5°C Upper test threshold of the humidity: 80°C Lower test threshold of the humidity: -20°C
External extended digital parameters	Digital parameter ID: 0-6 This digital parameter is set according to the actual requirements.

NOTE

The preceding data is configured according to the actual requirements. When the actually planned value of a parameter is the same as the default value, it is not necessary to configure the parameter.

Configuration Example

The following considers the configuration plan of the Power3000 as an example to describe the process of configuring the environment monitoring parameters of the Power3000.

```
huawei(config)#emu add 0 POWER3000 0 0 POWER3000
huawei(config)#display emu 0
huawei(config)#interface emu 0
huawei(config-if-power3000-0)#display power system parameter
huawei(config-if-power3000-0)#display power environment parameter
huawei(config-if-power3000-0)#power battery parameter 1 0.15 60 65
huawei(config-if-power3000-0)#power battery-test auto-test permit 60
huawei(config-if-power3000-0)#power temperature-off battery-off-state permit
battery-off-temperature 53
huawei(config-if-power3000-0)#power environment temperature 68 -5 80 -20
huawei(config-if-power3000-0)#display power system parameter
huawei(config-if-power3000-0)#display power environment parameter
huawei(config-if-power3000-0)#quit
huawei(config)#save
```

1.3.16.10 Commissioning the EMU_TCU

This topic describes how to commission the TCU to ensure that it monitors and controls the temperature conditions of the heat exchanger according to the actual conditions.

Context

NOTE

Commissioning the TCU only when the device is installed in the outdoor cabinet scenario.

The TCU is used to monitor the running status of the heat exchanger and to set the heating start temperature or the heating stop temperature according to actual conditions to ensure the normal heat dissipation of the device.

When commissioning the TCU, pay attention to the following points:

- The TCU sub-nodes are numbered from 0 to 31.
- When the system is configured with multiple EMUs simultaneously, make sure that the sub-nodes do not conflict with each other.

Copyright © Huawei Technologies Co., Ltd.

Table 1-40 lists the default configuration of the TCU.

Table 1-40 Default configuration of the TCU

Parameter	Default Value
Sub-node	7

Procedure

Step 1 Run the **emu add** command to add a TCU. By default, the sub-node ID is 7.

NOTE

The TCU communicates with the MA5600T/MA5603T/MA5608T in the master node and sub-node mode. the DIP switches of the sub-nodes for the TCU not need to be set on site.

Step 2 Run the **interface emu** command to enter the TCU mode.

Step 3 Run the **tcu heat temperature** command to set the heating start temperature and the heating stop temperature of the heat exchanger.

- When the current temperature is lower than the heating start temperature, the heater starts heating. The default value of the heating start temperature is 5 °C.
- When the temperature after heating reaches the heating stop temperature, the heater automatically stops heating. The default value of the heating stop temperature is 25 °C.
- When setting the heating start/stop temperature for the heat exchanger, ensure that the heating start temperature is lower than the heating stop temperature.

Step 4 Run the **tcu temperature** command to set the high-temperature alarm threshold and the low-temperature alarm threshold of the heat exchanger.

- When the current temperature of the heat exchanger is higher than the high-temperature threshold, the excessively high temperature alarm is reported. The default value of the high-temperature threshold is 68 °C.
- When the current temperature of the heat exchanger is lower than the low-temperature threshold, the excessively low temperature alarm is reported. The default value of the low-temperature threshold is -20°C.

Step 5 Run the **save** command to save the data.

----End

Result

- In the TCU mode, run the **display tcu system parameter** command to query the parameter configuration of the heat exchanger and ensure that the configuration is the same as the data plan.
- In the TCU mode, run the **display tcu environment info** command to query the running status of the heat exchanger and ensure that it is the same as the data plan.
- In the TCU mode, run the **display tcu alarm** command to query the alarm information reported by the TCU. The status of all the heat exchanger alarms is normal.

Copyright © Huawei Technologies Co., Ltd.

Example

To add a TCU (emuid: 2; sub-node: 7), and set the heating start temperature to -10°C and the heating stop temperature to 30°C for heat exchanger 2, do as follows:

```
huawei(config)#emu add 2 TCU 0 7 tcu

huawei(config)#interface emu 2

huawei(config-if-tcu-2)#tcu heat temperature

{ start-temperature<F><-90,40> }:-10
{ end-temperature<F><-90,40> }:30

  Command:
          tcu heat temperature -10 30
  Send command to environment monitor board ,please wait for a moment

huawei(config-if-tcu-2)#
  Execute command successful
```

1.3.16.11 Commissioning the EMU_FAN

This topic describes how to commission the FAN to ensure that it monitors the environmental conditions of the fans of the device according to the actual conditions.

Context

NOTE

When the device is delivered, the EMU_FAN is correctly connected to the shelf. The connection need not be changed for the device commissioning. In certain cases, if the EMU needs to be configured in other shelves, reconnect the EMU. For details, see this topic.

The FAN is used to monitor the running status of the fans and to set the fan rotation speed according to actual conditions to ensure the normal heat dissipation of the device.

When commissioning the FAN, pay attention to the following points:

- The EMU sub-nodes are numbered from 0 to 31.
- When the system is configured with multiple EMUs simultaneously, make sure that the sub-nodes do not conflict with each other.
- It is recommended that you use the **auto** mode as the fan speed adjustment mode.

Table 1-41 lists the default configuration of the FAN.

Table 1-41 Default configuration of the FAN

Parameter	Default Value
Sub-node	1
Fan speed adjustment mode	Automatic
Whether to report the fan alarm	Permit

Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Set the DIP switches of the sub-nodes for the FAN. By default, the sub-node ID is 1.

NOTE

The FAN communicates with the MA5600T/MA5603T/MA5608T in the master node and sub-node mode. Therefore, the DIP switches of the sub-nodes for the FAN must be consistent with those for the MA5600T/MA5603T/MA5608T. For details about how to configure the DIP switches of the FAN, see the Description of DIP Switches in **1.3.1.2 Checking the Settings of DIP Switches on the Fan Monitoring Board**. The Description of DIP Switches in **1.3.1.2 Checking the Settings of DIP Switches on the Fan Monitoring Board** applies only to the MA5600T/MA5603T/MA5608T, but does not apply to the MA5608T.

Step 2 Insert the fan tray into the corresponding slot of the service shelf.

Step 3 Run the **emu add** command to add a FAN. By default, the sub-node ID is 1.

Step 4 Run the **interface emu** command to enter the FAN mode.

Step 5 Run the **fan speed mode auto** or **fan speed mode manual** command to set the fan speed adjustment mode. By default, the fan speed adjustment mode is automatic.

NOTE

When the fan speed adjustment mode is the manual mode, you can run the **fan speed mode manual** command to set the fan speed. The speed level can be 0, 1, 2, 3, 4, 5 or 6. Here, 6 stands for the highest level, and 0 stands for the lowest level.

Step 6 Run the **fan alarmset** command to configure the fan alarm reporting function. The fan alarms are read temperature failure alarm, fan block alarm, over temperature alarm, and power fault alarm. By default, the fan alarm reporting is permitted.

Step 7 Run the **save** command to save the data.

----End

Result

- In the FAN mode, run the **display fan system parameter** command to query the parameter configuration of the fan tray and ensure that the configuration is the same as the data plan.
- In the FAN mode, run the **display fan environment info** command to query the running status of the fan tray and ensure that it is the same as the data plan.
- In the FAN mode, run the **display fan alarm** command to query the alarm information reported by the fan tray. The status of all the fan alarms is normal.

Example

To add a FAN, and adopt the default settings for the speed adjustment mode and alarm function, do as follows:

```
huawei(config)#emu add 0 FAN 0 1 FAN

huawei(config)#interface emu 0

huawei(config-if-fan-0)#display fan system parameter

  EMU ID: 0
  FAN configration parameter:
  --------------------------------------------------------------------------
  FAN timing mode: Auto timing by temperature
  --------------------------------------------------------------------------
  Alarm_name                        Permit/Forbid
```


Copyright © Huawei Technologies Co., Ltd.

```
Read temperature fault                Permit
Fan block                             Permit
Temperature high                      Permit
Power fault                           Permit
------------------------------------------------------------------------------
```

1.3.17 Saving and Backing Up Data

The MA5600T/MA5603T/MA5608T supports data saving and backup to upgrade the system or to recover the system in case of an upgrade failure or any other critical events.

1.3.17.1 Manually Saving and Backing Up Data

This topic describes how to manually save data to the flash memory or back up data to the server in case of data loss caused by an unexpected system restart.

Prerequisites

The file transfer mode is configured. For detailed configurations, see

- **Configuring the FTP Transfer Mode**
- **Configuring the SFTP Transfer Mode**
- **Configuring the TFTP Transfer Mode**

NOTE

You need to configure only one of the above-mentioned three file transfer modes. You are advised to use SFTP mode.

Procedure

- Manually save data.

  System data files are saved manually.

  The system data files include the database file and the configuration file. **Table 1-42** lists the commands for manually saving the data files and describes command functions.

  Table 1-42 List of commands for manually saving the data files

Operation	Command	Function
Manually save the database file	**save data**	Saves only the database file but not the configuration file.
Manually save the configuration file	**save configuration**	Saves only the configuration file but not the database file.
Manually save the database file and the configuration file	**save**	Saves the database file and the configuration file.

Copyright © Huawei Technologies Co., Ltd.

- Select one of the saving modes in **Table 1-42** to manually save the system data files according to the actual requirements.

- Manually back up data.

  System data files are backed up manually.

  Prerequisite

  - Data is saved. For detailed configurations, see **Manually save data**.

  The system data files include the database file and the configuration file. **Table 1-43** lists the commands for manually backing up the data files and describes command functions.

  Table 1-43 List of commands for manually backing up the data files

Operation	Command	Function
Manually back up the database file	**backup data**	● Manually backs up the database file to the server. ● The IP address of the server where the backup files are stored must be identical to the one configured in the FTP/ SFTP/TFTP tool. The file name must be specified.
Manually back up the configuration file	**backup configuration**	● Manually backs up the configuration file to the server. ● The IP address of the server where the backup files are stored must be identical to the one configured in the FTP/ SFTP/TFTP tool. The file name must be specified.

  - Select one of the backup modes in **Table 1-43** to manually back up the system data according to the actual requirements.

----End

Result

1. The system displays a message indicating that the database file and the configuration file have been saved successfully.

Copyright © Huawei Technologies Co., Ltd.

2. After the backup is completed, you can locate the file backed up in the path that you set in the FTP tool.

Example

Manually saving data

Select one of the following modes to save the database file or the configuration file.

- To save the database file in the system, do as follows:

```
huawei(config)#save data
  The data is being saved, please wait a moment...

huawei(config)#
  1 [2010-07-12 14:32:00+08:00]:The percentage of saved data on 9 slot's main
control board is: 21%

huawei(config)#
  1 [2010-07-12 14:32:03+08:00]:The percentage of saved data on 9 slot's main
control board is: 27%

huawei(config)#
  1 [2010-07-12 14:32:06+08:00]:The percentage of saved data on 9 slot's main
control board is: 66%

huawei(config)#
  1 [2010-07-12 14:32:09+08:00]:The percentage of saved data on 9 slot's main
control board is: 72%

huawei(config)#
  1 [2010-07-12 14:32:12+08:00]:The percentage of saved data on 9 slot's main
control board is: 96%

huawei(config)#
  1 [2010-07-12 14:32:15+08:00]:The percentage of saved data on 9 slot's main
control board is: 98%

huawei(config)#
  1 [2010-07-12 14:32:18+08:00]:The percentage of saved data on 9 slot's main
control board is: 98%

huawei(config)#

huawei(config)#
  1 [2010-07-12 14:32:19+08:00]:The data of 9 slot's main control board is
saved
 completely
```

- To save the configuration file in the system, do as follows:

```
huawei#save configuration

huawei#
  It will take several minutes to save configuration file, please wait...

huawei#
  Configuration file had been saved successfully
  Note: The configuration file will take effect after being activated
```

- To save the database file and the configuration file in the system, do as follows:

```
WS6803(config)#save
{ <cr>|configuration<K>|data<K> }:

  Command:
          save

huawei(config)#
```


Copyright © Huawei Technologies Co., Ltd.

```
  It will take several minutes to save configuration file, please wait...

huawei(config)#
  Configuration file had been saved successfully
  Note: The configuration file will take effect after being activated

huawei(config)#
  The data is being saved, please wait a moment...

huawei(config)#
  1 [2010-07-12 14:35:05+08:00]:The percentage of saved data on 9 slot's main
control board is: 21%

huawei(config)#
  1 [2010-07-12 14:35:08+08:00]:The percentage of saved data on 9 slot's main
control board is: 27%

huawei(config)#
  1 [2010-07-12 14:35:11+08:00]:The percentage of saved data on 9 slot's main
control board is: 66%

huawei(config)#
  1 [2010-07-12 14:35:14+08:00]:The percentage of saved data on 9 slot's main
control board is: 72%

huawei(config)#
  1 [2010-07-12 14:35:17+08:00]:The percentage of saved data on 9 slot's main
control board is: 78%

huawei(config)#
  1 [2010-07-12 14:35:20+08:00]:The percentage of saved data on 9 slot's main
control board is: 96%

huawei(config)#
  1 [2010-07-12 14:35:23+08:00]:The percentage of saved data on 9 slot's main
control board is: 98%

huawei(config)#

huawei(config)#
  1 [2010-07-12 14:35:25+08:00]:The data of 9 slot's main control board is
saved
 completely
```

Manually backing up data

1. For configuring and enabling the FTP tool on the backup sever, see **Configuring the FTP Transfer Mode**.
2. Select one of the following modes to back up the database file or the configuration file to the server.
   - Assume that the IP address of the backup server is 10.10.10.1 and the database file name is data0.dat. To back up the database file to the backup server through FTP, do as follows:

```
huawei(config)#backup data ftp 10.10.10.1 data0.dat

Command:
          backup data tftp 10.10.10.1
data0.dat
  Please save database file before backup, or the database file that is
backed
up may be not the lastest one. Are you sure to continue? (y/n)[n]: y
  Load(backup,duplicate,...) begins, please wait and notice the rate of
progress
  Any operation such as reboot or switchover will cause failure and
unpredictable result
```


Copyright © Huawei Technologies Co., Ltd.

```
  Backing up files starts from the host to the maintenance terminal
  PARAMETERS :FrameID: 0, SlotID: 9, Position: -1, Backup type: Host data,
Backup Object: Active control board

huawei(config)#

huawei(config)#
  Backing up files is successful from the host to the maintenance terminal
  PARAMETERS :FrameID: 0, SlotID: 9, Position: -1, Backup type: Host data,
Backup Object: Active control board
```

- Assume that the IP address of the backup server is 10.10.10.1 and the configuration file name is config0.txt. To back up the configuration file to the backup server through FTP, do as follows:

```
huawei(config)#backup configuration ftp 10.10.10.1 config0.txt
  Please save configuration file before backup, or the configuration
file
backuped may be not the lastest. Are you sure to continue? (y/n)[n]:
y
  Load(backup,duplicate,...) begins, please wait and notice the rate of
progress
  Any operation such as reboot or switchover will cause failure and
unpredictable result
  Backing up files starts from the host to the maintenance terminal
  PARAMETERS :FrameID: 0, SlotID: 9, Position: -1, Backup type:
Configuration
file, Backup Object: Active control board

huawei#

huawei#
  Backing up files is successful from the host to the maintenance terminal
  PARAMETERS :FrameID: 0, SlotID: 9, Position: -1, Backup type:
Configuration
file, Backup Object: Active control board
```

1.3.17.2 Configuring the Auto-save and Auto-backup Functions

This topic describes how to configure the auto-save and auto-backup functions so that data is automatically saved in the flash memory or backed up to the server. These functions ensure that data or configuration files are not lost after emergency restart.

Prerequisites

The file transfer mode is configured. For details, see the following descriptions.

- **Configuring the FTP File Transfer Mode**
- **Configuring the FTP File Transfer Mode**
- **Configuring the TFTP File Transfer Mode**

NOTE

You need to configure only one of the above-mentioned three file transfer modes. You are advised to use SFTP mode.

Procedure

Step 1 Configure the auto-save function and an auto-backup server.

- Configure the auto-save function

  If the auto-save function is enabled, the system periodically checks whether data is modified at the preset time or at a preset interval. If data is modified, the system automatically saves the modified data. Otherwise, the system does not perform the auto-save operation.

Copyright © Huawei Technologies Co., Ltd.

Data to be saved includes database files and configuration files. **Table 1-44** lists the commands and functions of auto-save operations.

Table 1-44 Auto-save operations

Auto-save	Command	Function
Set the auto-save file type.	**autosave type { all | configuration | data }**	● data: Saves only database files. ● configuration: Saves only configuration files. ● all: Saves both database files and configuration files.
Save database files automatically at the preset time.	**autosave time**	● The system saves data at the preset time. ● By default, the system automatically saves data at 00:00:00 every day.
Save database files automatically at an interval.	**autosave interval**	● The system automatically saves data at a preset interval. ● By default, the system saves database files at an interval of 30 minutes.

NOTE

- By default, the **autosave interval** function is disabled in the system. That is, the system does not automatically save data. Hence, you need to manually save data.
- When the **autosave interval** function is enabled, you still can manually save data.
- If data is saved frequently, the system will be affected. Therefore, it is suggested that you set the auto-save interval to longer than 60 minutes. It is better to set the auto-save interval to equal to or longer than one day.
- Before upgrading the system, run the **autosave interval***off* or **autosave time***off* command to disable the auto-save function to prevent upgrade failure due to the conflict between upgrade and auto-save operations.

NOTICE

After the system upgrade is complete, you must re-enable the auto-save function if the auto-save function is required.

- Configure an auto-backup server.

  An auto-backup server backs up data, configuration, and logs of a device to an external server. After an auto-backup server is configured, you can configure the auto-backup function.

Copyright © Huawei Technologies Co., Ltd.

Auto-backup servers are classified into an active auto-backup server and standby auto-backup server.

- You can configure only an active auto-backup server or you can configure active and standby auto-backup servers to ensure that data is backed up.
- When the active auto-backup server does not work properly, data is automatically backed up to the standby auto-backup server.

Run the **file-server autobakup** command to configure the active and standby auto-backup servers for backing up data, configuration, and logs.

NOTE

The file transfer mode, user name, and password configured must be the same as those of xFTP.

Step 2 Configure the auto-backup function.

The database files, configuration files, and logs in the system are automatically backed up to a specified external server.

Table 1-45 lists the commands and functions of auto-backup operations.

Table 1-45 Auto-backup operations

Auto-backup	Command	Function
Back up database files automatically.	**auto-backup manual data**	Immediately and automatically back up database files to the auto-backup server.
	● **auto-backup period data interval** ● **auto-backup period data enable**	● Automatically back up database files to the auto-backup server at an interval. ● Set the interval and start time of automatically backing up database files and then enable the auto-backup function for database files.
Back up configuration files automatically.	**auto-backup manual configuration**	Immediately and automatically back up configuration files to the auto-backup server.
	● **auto-backup period configuration interval** ● **auto-backup period configuration enable**	● Automatically back up configuration files to the auto-backup server at an interval. ● Set the interval and start time of automatically backing up configuration files and then enable the auto-backup function for configuration files.

Copyright © Huawei Technologies Co., Ltd.

Auto-backup	Command	Function
Back up logs.	● **auto-backup period log interval** ● **auto-backup period log enable**	Set the interval and start time of automatically backing up logs and then enable the auto-backup function for logs.

----End

Result

1. After the auto-save function is configured, run the **display autosave configuration** command to query the preset time and preset interval.
2. After the auto-backup server is configured, run the **display file-server auto-backup** command to query configuration information about the file server, including server type, file transfer mode, IP address, user name, and password (the last three parameters are for only FTP and SFTP).
3. After the auto-backup function is configured, you can browse backup files in the path that files configured in xFTP are saved to. The file names are assigned by the system.

Example

Configure the auto-save function.

1. Configure the type of auto-save data, including database files and configuration files.
```
huawei(config)#autosave
type
{ all<K>|configuration<K>|
data<K> }:all


Command:
          autosave type all
```
2. Configure the auto-save function at a specified time or at a preset interval.
   - Set the auto-save time at 02:00:00 and enable the auto-save function.
```
huawei(config)#autosave time
02:00:00
  System autosave time switch:
off
  Autosave time:
02:00:00
  Autosave type: data and configuration file

huawei(config)#autosave time
on
  System autosave time switch:
on
  Autosave time:
02:00:00
  Autosave type: data and configuration file
```
   - Set the auto-save interval to 1440 minutes and enable the **autosave interval** function. The system checks whether the configuration data is modified every 1440 minutes. If the configuration data is modified, the system automatically saves the modified configuration. Otherwise, the system does not perform the auto-save operation.

Copyright © Huawei Technologies Co., Ltd.

NOTICE

The **autosave interval** command conflicts with the **autosave time** command. You can use either of the commands to enable the auto-save function. To switch from one function to the other one, you need to disable the enabled function first.

```
huawei(config)#autosave interval
1440
  System autosave interval switch:
off
  Autosave interval: 1440
minutes
  Autosave type: data and configuration file

huawei(config)#autosave interval
on
  System autosave interval switch:
on
  Autosave interval: 1440
minutes
  Autosave type: data and configuration
file

  System autosave modified configuration switch:
on
  Autosave interval: 30
minutes
  Autosave type: data and configuration file
```

Configure the auto-backup function.

1. Select any of the following modes to back up database files, configuration files, and logs to the backup server.
   - To enable the auto-backup function for the database file, and set the auto-backup interval to one day and the start time to 02:30, do as follows:
     ```
     huawei(config)#auto-backup period data interval 1 time 02:30
     huawei(config)#auto-backup period data enable
     ```
   - To enable the auto-backup function for the configuration file, and set the auto-backup interval to one day and the start time to 03:30, do as follows:
     ```
     huawei(config)#auto-backup period configuration interval 1 time 03:00
     huawei(config)#auto-backup period configuration enable
     ```
   - To enable the auto-backup function for the logs, and set the auto-backup interval to one day and the start time to 06:00, do as follows:
     ```
     huawei(config)#auto-backup period log interval 1 time 06:00
     huawei(config)#auto-backup period log enable
     ```

1.4 Interconnection Commissioning

The MA5600T/MA5603T/MA5608T provides multiple interfaces for interconnection. This topic describes the interconnection commissioning of the MA5600T/MA5603T/MA5608T. The following recommended commissioning tasks and sequences are for reference only. Different offices have different conditions; therefore, it is recommended that customers, with the assistance of Huawei engineers, modify commissioning tasks according to actual requirements.

Copyright © Huawei Technologies Co., Ltd.

1.4.1 Commissioning the Interconnection with the NMS

The MA5600T/MA5603T/MA5608T provides the function of interconnecting with the network management system, with which the administrator can maintain and manage the MA5600T/MA5603T/MA5608T through the NMS. This topic considers the iManager U2000 Network Management System (hereinafter referred to as the U2000) as an example to describe how to perform the interconnection commissioning between the U2000 and the MA5600T/MA5603T/MA5608T in the inband mode and the outband mode. SNMPv3 has higher security than SNMPv1 and SNMPv2c. Therefore, it is recommended.

1.4.1.1 Commissioning Outband Network Management (SNMP V1 and V2)

This topic describes how to implement the outband network management on the MA5600T/MA5603T/MA5608T using the local maintenance Ethernet port (outband network management port). This enables the U2000 to maintain the MA5600T/MA5603T/MA5608T using this management channel. In the outband network management mode, a non-service channel is used to transmit the management information. With the use of the non-service channel, the management channel is separated from the service channel, which is more reliable than in the inband network management mode.

Service Requirements

In the network as shown in **Figure 1-49**, the service requirements are as follows:

- The MA5600T/MA5603T/MA5608T provides the outband network management channel using the local maintenance Ethernet port.
- A static route is used between the MA5600T/MA5603T/MA5608T and the U2000.

Figure 1-49 Example network for the outband network management

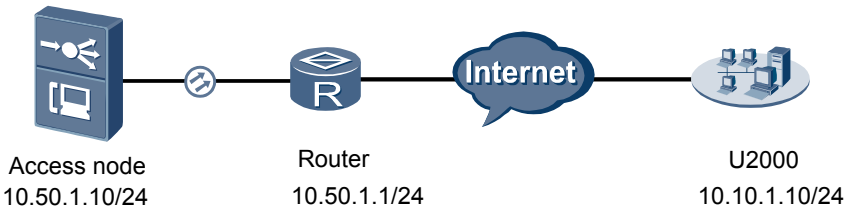
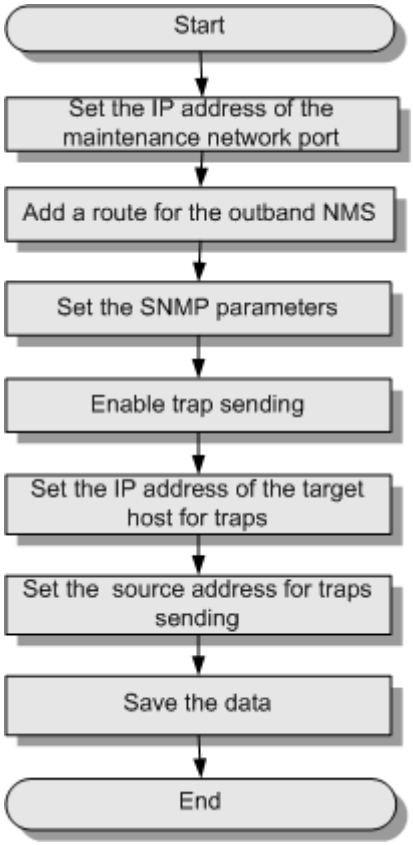


Figure 1-50 shows the flowchart for commissioning the outband network management on the device.

Copyright © Huawei Technologies Co., Ltd.

Figure 1-50 Flowchart for commissioning the outband network management on the device



Procedure

- Commission the outband network management on the device.
  1. Configure the IP address of the maintenance Ethernet port.

     The IP address of the local maintenance Ethernet port (outband network management port) of the MA5600T/MA5603T/MA5608T is 10.50.1.10/24.

     NOTE

     By default, the IP address of the maintenance Ethernet port (ETH port on the control board) is 10.11.104.2, and the subnet mask is 255.255.255.0.

     ```
     huawei(config)#interface meth 0
     huawei(config-if-meth0)#ip address 10.50.1.10 255.255.255.0
     huawei(config-if-meth0)#quit
     ```

  2. Add a route for the outband network management.

     Use the static route. The destination IP address is 10.10.1.0/24 (the network segment to which the U2000 belongs), and the gateway IP address is 10.50.1.1/24 (the IP address of the gateway of the MA5600T/MA5603T/MA5608T).

     ```
     huawei(config)#ip route-static 10.10.1.0 24 10.50.1.1
     ```

  3. Set the SNMP parameters.

     a. Configure the community name and the access authority.

     The read community name is **public**, and the write community name is **private**.

Copyright © Huawei Technologies Co., Ltd.

NOTE

The configurations of the read community name and the write community name must be the same as the configurations on the U2000.

```
huawei(config)#snmp-agent community read public
huawei(config)#snmp-agent community write private
```

b. (Optional) Set the ID and the contact means of the administrator.

The contact means of the administrator is **HW-075528780808**.

```
huawei(config)#snmp-agent sys-info contact HW-075528780808
```

c. (Optional) Set the location of the device.

The location of the device is **Shenzhen_China**.

```
huawei(config)#snmp-agent sys-info location Shenzhen_China
```

d. Set the SNMP version.

- The SNMP version is SNMP V1.

```
huawei(config)#snmp-agent sys-info version v1
```

- The SNMP version is SNMP V2.

```
huawei(config)#snmp-agent sys-info version v2c
```

NOTE

The SNMP version must be the same as the SNMP version set on the U2000.

4. Enable the function of sending traps.

On the MA5600T/MA5603T/MA5608T, enable the function of sending traps to the U2000.

```
huawei(config)#snmp-agent trap enable standard
```

5. Configure the IP address of the destination host for the traps.

- When the SNMP V1 is used, the host name is **huawei**, the IP address of the host is **10.10.1.10/24** (IP address of the U2000), the trap parameter name is **ABC**, SNMP version is **V1**, and the parameter security name is **private** (the parameter security name is the SNMP community name).

```
huawei(config)#snmp-agent target-host trap-hostname huawei address
10.10.1.10
 trap-paramsname ABC
huawei(config)#snmp-agent target-host trap-paramsname
 ABC v1 securityname private
```

- When the SNMP V2 is used, the host name is **huawei**, the IP address of the host is **10.10.1.10/24** (IP address of the U2000), the trap parameter name is **ABC**, SNMP version is **V2**, and the parameter security name is **private** (the parameter security name is the SNMP community name).

```
huawei(config)#snmp-agent target-host trap-hostname huawei address
 10.10.1.10 trap-paramsname ABC
huawei(config)#snmp-agent target-host trap-paramsname ABC
 v2c securityname private
```

6. Set the IP address of the maintenance Ethernet port as the source IP address for sending traps.

Set the SNMP packets to be forwarded from the maintenance Ethernet port of the MA5600T/MA5603T/MA5608T. That is, the source address of the traps is meth 0.

```
huawei(config)#snmp-agent trap source meth 0
```

7. Save the data.

```
huawei(config)#save
```


Copyright © Huawei Technologies Co., Ltd.

- Commission the outband network management on the U2000.
  1. Configure the gateway of the route from the U2000 to network segment 10.50.1.0/24 to 10.10.1.1.
     - In the Solaris OS, do as follows:

       Run the **route add 10.50.1.0 10.10.1.1** command to add a route.

       Run the **netstat -r** command to query the information about the current routing table.
     - In the Windows OS, do as follows:

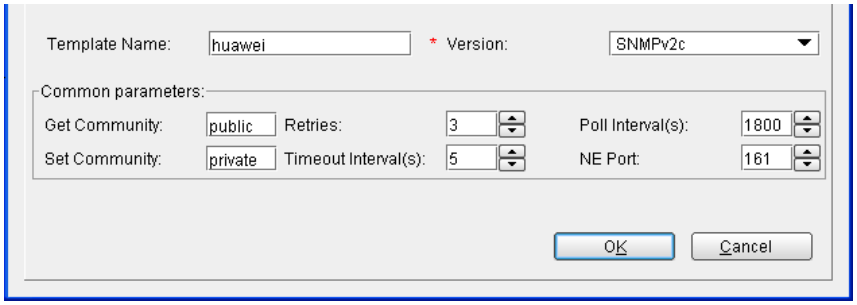
       Run the **route add 10.50.1.0 mask 255.255.255.0 10.10.1.1** command to add a route.

       Run the **route print** command to query the information about the current routing table.

     NOTE

     If the IP address of the outband network management port and the IP address of the U2000 are in the same network segment, you need not configure the routing information.
  2. Log in to the U2000.
  3. Set the SNMP parameters. A default SNMP profile exists in the system. Use the default profile in this service. If a new profile is required, do as follows:
     a. Choose **Administration** > **NE Communicate Parameter** > **Default Access Protocol Parameters** from the main menu.
     b. - When the SNMP V1 is used, choose **SNMP v1 Parameter** on the **Default Access Protocol Parameters** tab page. Then click **Add** and set the SNMP parameters, as shown in the following figure (the other parameters except **Profile name** use the default settings).

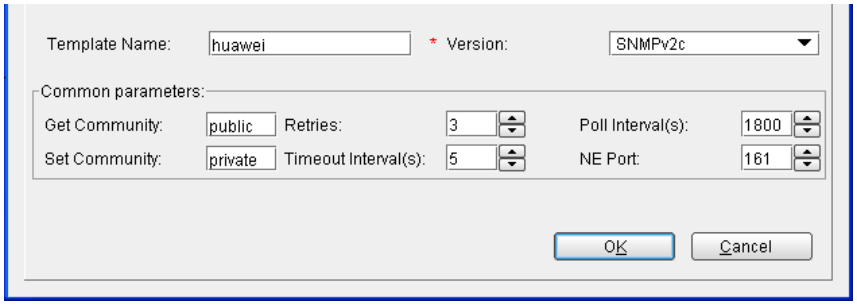
        Figure 1-51 Set the SNMP parameters

        - When the SNMP V2 is used, choose **SNMP v2 Parameter** on the **Default Access Protocol Parameters** tab page. Then click **Add** and set the SNMP parameters, as shown in the following figure (the other parameters except **Profile name** use the default settings).

Copyright © Huawei Technologies Co., Ltd.

Figure 1-52 Set the SNMP parameters



NOTE

The configurations of **Get Community** and **Set Community** are the same as the configurations on the MA5600T/MA5603T/MA5608T.

c. Click **OK**.

d. Select the added SNMP parameters. Click **OK**.

e. In the dialog box that is displayed, click **Yes** to test the set SNMP parameters.

f. The U2000 displays the **Loading** dialog box. After the testing is complete, click **OK**.

4. Add a device.

a. In the **Physical Root** navigation tree on the **Main Topology** tab page, right-click and choose **New** > **NE** from the shortcut menu.

b. In the dialog box that is displayed, choose **Access NE** > **Access NE** from the main menu.

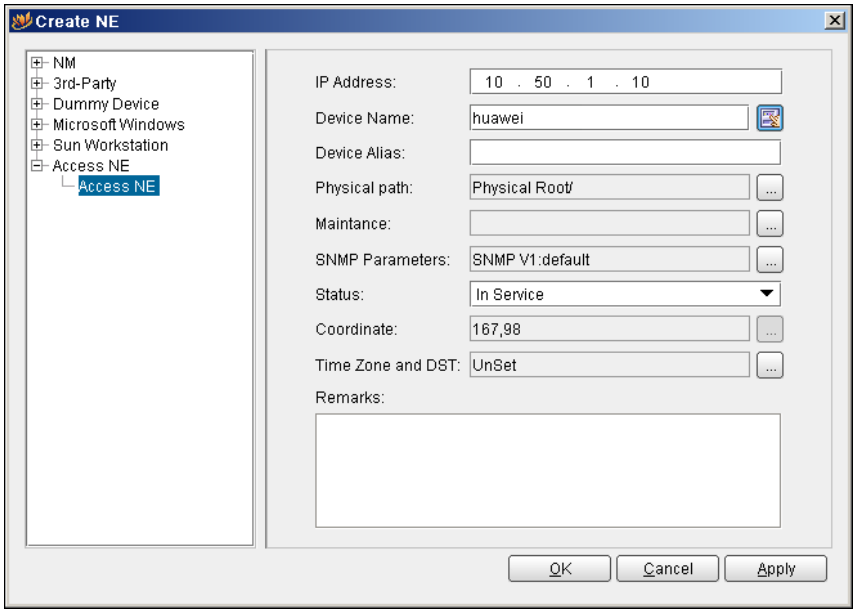
c. In the right pane, set the parameters.

- When the SNMP V1 is used, In the dialog box that is displayed, set the required parameters, as shown in the following figure.

  IP Address is **10.50.1.10**, **Device Name** is **huawei**, and **SNMP Parameters** is **SNMP V1:default**.

Copyright © Huawei Technologies Co., Ltd.

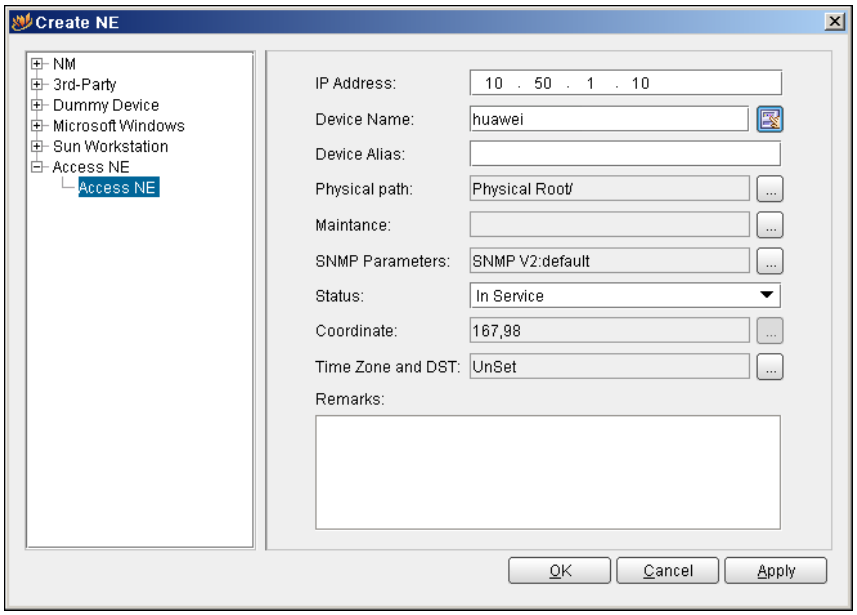
Figure 1-53 Add device



- When the SNMP V2 is used, In the dialog box that is displayed, set the required parameters, as shown in the following figure.

  IP Address is **10.50.1.10**, **Device Name** is **huawei**, and **SNMP Parameters** is **SNMP V2:default**.

Figure 1-54 Add device



Copyright © Huawei Technologies Co., Ltd.

d. Click **OK**. The system displays a message indicating that several seconds or some 10 minutes are required for uploading the device data. After the related data is read, the system automatically refreshes and displays the device icon.

----End

Result

You can maintain and manage the MA5600T/MA5603T/MA5608T using the U2000.

Configuration File

The following describes the script for commissioning the outband network management on the device (SNMP V1).

```
interface meth 0
ip address 10.50.1.10 255.255.255.0

quit
ip route-static 10.10.1.0 24 10.50.1.1

snmp-agent community read public

snmp-agent community write private

snmp-agent sys-info contact HW-075528780808
snmp-agent sys-info location Shenzhen_China
snmp-agent sys-info version v1

snmp-agent trap enable standard
snmp-agent target-host trap-hostname huawei address 10.10.1.10 trap-paramsname ABC
snmp-agent target-host trap-paramsname ABC v1 securityname private

snmp-agent trap source meth 0

save
```

The following describes the script for commissioning the outband network management on the device (SNMP V2).

```
interface meth 0
ip address 10.50.1.10 255.255.255.0

quit
ip route-static 10.10.1.0 24 10.50.1.1

snmp-agent community read public

snmp-agent community write private

snmp-agent sys-info contact HW-075528780808
snmp-agent sys-info location Shenzhen_China
snmp-agent sys-info version v2c

snmp-agent trap enable standard
snmp-agent target-host trap-hostname huawei address 10.10.1.10 trap-paramsname ABC
snmp-agent target-host trap-paramsname ABC v2c securityname private

snmp-agent trap source meth 0

save
```


Copyright © Huawei Technologies Co., Ltd.

1.4.1.2 Commissioning Outband Management (SNMP V3)

This topic describes how to implement the outband network management on the MA5600T/MA5603T/MA5608T using the local maintenance Ethernet port (outband network management port). This enables the U2000 to maintain the MA5600T/MA5603T/MA5608T using this management channel. In the outband network management mode, a non-service channel is used to transmit the management information. With the use of the non-service channel, the management channel is separated from the service channel, which is more reliable than in the inband network management mode.

Service Requirements

In the network as shown in **Figure 1-55**, the service requirements are as follows:

- The MA5600T/MA5603T/MA5608T provides the outband network management channel through the local maintenance Ethernet port.
- A static route is used between the MA5600T/MA5603T/MA5608T and the U2000.
- SNMP V3 is used (more reliable than V1 and V2, providing network security and access control management functions).

Figure 1-55 Example network for the outband network management

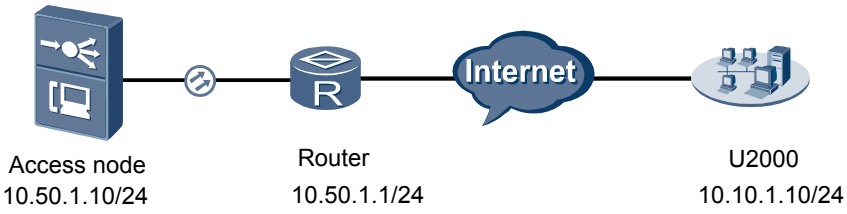
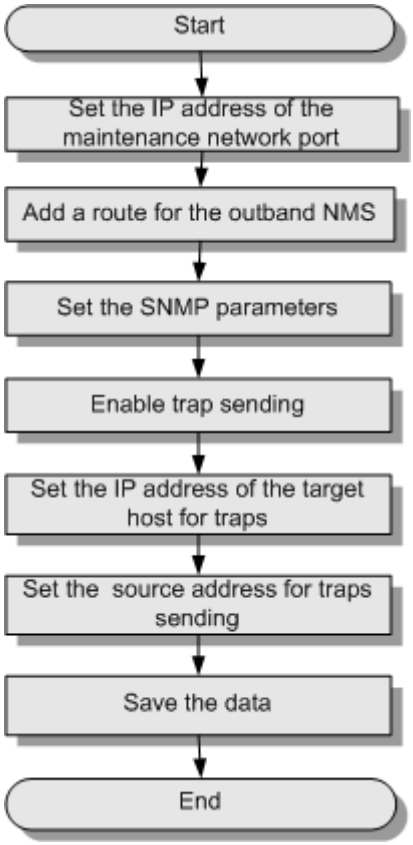


Figure 1-56 shows the flowchart for commissioning the outband network management on the device.

Copyright © Huawei Technologies Co., Ltd.

Figure 1-56 Flowchart for commissioning the outband network management on the device



Procedure

- Commission the outband network management on the device.
  1. Configure the IP address of the maintenance Ethernet port.

     The IP address of the local maintenance Ethernet port (outband network management port) of the MA5600T/MA5603T/MA5608T is 10.50.1.10/24.

     NOTE

     By default, the IP address of the maintenance Ethernet port (ETH port on the control board) is 10.11.104.2, and the subnet mask is 255.255.255.0.

     ```
     huawei(config)#interface meth 0
     huawei(config-if-meth0)#ip address 10.50.1.10 255.255.255.0
     huawei(config-if-meth0)#quit
     ```

  2. Add a route for the outband network management.

     Use the static route. The destination IP address is 10.10.1.0/24 (the network segment to which the U2000 belongs), and the gateway IP address is 10.50.1.1/24 (the IP address of the gateway of the MA5600T/MA5603T/MA5608T).

     ```
     huawei(config)#ip route-static 10.10.1.0 24 10.50.1.1
     ```

  3. Set the SNMP parameters.

     a. Configure the SNMP user, group, and view.

     The user name is **user1**, the group name is **group1**, the user authentication mode is **SHA**, the authentication password is **authkey123**, the user encryption mode

Copyright © Huawei Technologies Co., Ltd.

is **aes128**, the encryption password is **prikey123**, the read and write view names are **hardy**, and the view includes the internet subtree.

```
huawei(config)#snmp-agent usm-user v3 user1 group1
authentication-mode sha authkey123 privacy-mode aes128 prikey123
huawei(config)#snmp-agent group v3 group1 privacy read-view hardy
write-view hardy
huawei(config)#snmp-agent mib-view hardy include internet
```

NOTE

AES128 is recommended because it has higher security than DES56.

b. (Optional) Set the ID and contact means of the administrator.

The contact means of the administrator is **HW-075528780808**.

```
huawei(config)#snmp-agent sys-info contact HW-075528780808
```

c. (Optional) Set the location of the device.

The location of the device is **Shenzhen_China**.

```
huawei(config)#snmp-agent sys-info location Shenzhen_China
```

d. (Optional) Configure the engine ID of the SNMP entity.

The engine ID of the SNMP entity is set to 0123456789.

NOTE

The context engine ID of the SNMP must be the same as that on the U2000.

```
huawei(config)#snmp-agent local-engineid 0123456789
```

e. Set the SNMP version.

The SNMP version is SNMP V3.

NOTE

The SNMP version must be the same as the SNMP version set on the U2000.

```
huawei(config)#snmp-agent sys-info version v3
```

4. Enable the function of sending traps.

On the MA5600T/MA5603T/MA5608T, enable the function of sending traps to the U2000.

```
huawei(config)#snmp-agent trap enable standard
```

5. Configure the IP address of the destination host for the traps.

The host name is **huawei**, the IP address of the host is **10.10.1.10/24** (IP address of the U2000), the trap parameter name is **ABC**, the SNMP version is **V3**, the parameter security name is **user1** (when the SNMP V3 is used, the parameter security name is the USM user name), and the traps are authenticated and encrypted.

```
huawei(config)#snmp-agent target-host trap-hostname huawei
address 10.10.1.10 trap-paramsname ABC
huawei(config)#snmp-agent target-host trap-paramsname
ABC v3 securityname user1 privacy
```

6. Set the IP address of the maintenance Ethernet port as the source IP address for sending traps.

Set the SNMP packets to be forwarded from the maintenance Ethernet port of the MA5600T/MA5603T/MA5608T. That is, the source address of the traps is meth 0.

```
huawei(config)#snmp-agent trap source meth 0
```

7. Save the data.

```
huawei(config)#save
```

- Commission the outband network management on the U2000.

Copyright © Huawei Technologies Co., Ltd.

1. Configure the gateway of the route from the U2000 server to network segment 10.50.1.0/24 to 10.10.1.1.
   - In the Solaris OS, do as follows:

     Run the **route add 10.50.1.0 10.10.1.1** command to add a route.

     Run the **netstat -r** command to query the information about the current routing table.
   - In the Windows OS, do as follows:

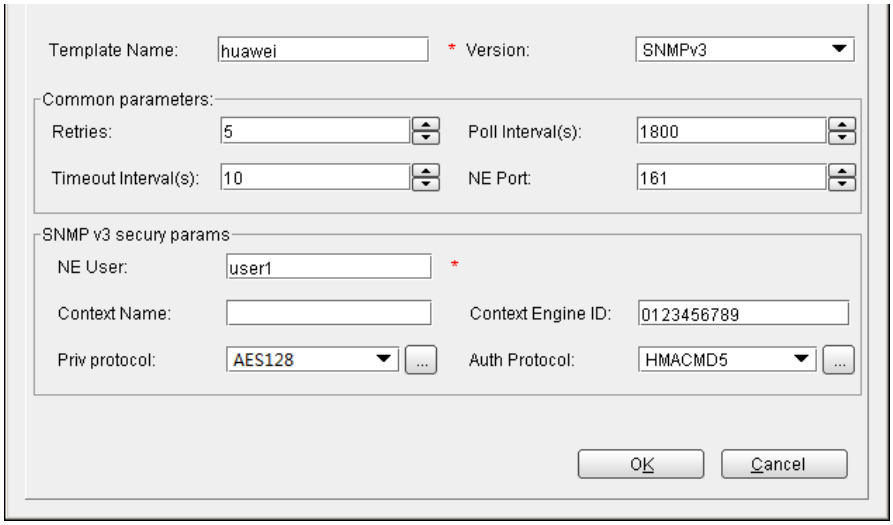
     Run the **route add 10.50.1.0 mask 255.255.255.0 10.10.1.1** command to add a route.

     Run the **route print** command to query the information about the current routing table.

   NOTE

   When the IP address of the network management port and the IP address of the U2000 are in the same network segment, you need not configure the routing information.
2. Set the SNMP parameters.
   a. Choose **Administration** > **NE Communicate Parameter** > **Default Access Protocol Parameters** from the main menu.
   b. Choose **SNMP v3 Parameter** on the **Default Access Protocol Parameters** tab page. Then click **Add** and set the SNMP parameters, as shown in **Figure 1-57**.

      Figure 1-57 Set the SNMP parameters

      After selecting corresponding protocols in **Priv Protocol** and **Auth Protocol**, click ... next to the parameter, and set the passwords of data encryption protocol and authentication protocol, as shown in **Figure 1-58**.

Copyright © Huawei Technologies Co., Ltd.

Figure 1-58 Set the password

NOTE

NE User, **Context Engine ID**, **Priv Protocol** and password, and **Auth Protocol** and password must be the same as those configured on the MA5600T/MA5603T/MA5608T. You can run the **display snmp-agent usm-user** command to query the device user, data encryption protocol, and authentication protocol on the MA5600T/MA5603T/MA5608T and run the **display snmp-agent local-engineid** command to query the context engine ID on the MA5600T/MA5603T/MA5608T.

c. Click **OK**.

d. Select the added SNMP parameters. Click **OK**.

e. In the dialog box that is displayed, click **Yes** to test the set SNMP parameters.

f. The U2000 displays the **Loading** dialog box. After the testing is complete, click **OK**.

3. Add a device.

a. In the **Physical Root** navigation tree on the **Main Topology** tab page, right-click and choose **New** > **NE** from the shortcut menu.

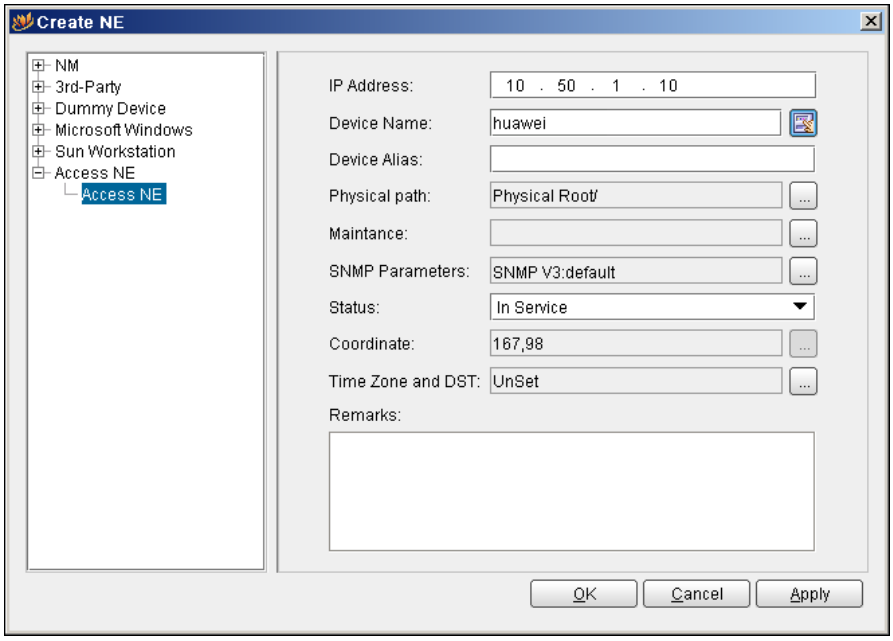
b. In the dialog box that is displayed, choose **Access NE** > **Access NE** from the main menu.

c. In the dialog box that is displayed, set the required parameters, as shown in **Figure 1-59**.

IP address is **10.50.1.10**, **Device Name** is **huawei**, **SNMP Parameters** is **SNMP V3:default**.

Copyright © Huawei Technologies Co., Ltd.

Figure 1-59 Add device



4. Click **OK**. The system prompts a message indicating that several seconds or some 10 minutes are required for uploading the device data. After the related data is read, the system automatically refreshes and displays the device icon.

----End

Result

You can maintain and manage the MA5600T/MA5603T/MA5608T through the U2000.

Configuration File

The following describes the script for commissioning the outband network management on the device.

```
interface meth 0
ip address 10.50.1.10 255.255.255.0

quit
ip route-static 10.10.1.0 24 10.50.1.1
snmp-agent usm-user v3 user1 group1 authentication-mode sha authkey123 privacy-mode
aes128 prikey123
snmp-agent group v3 group1 privacy read-view hardy write-view hardy

snmp-agent mib-view hardy include internet

snmp-agent sys-info contact HW-075528780808
snmp-agent sys-info location Shenzhen_China
snmp-agent sys-info version v3

snmp-agent trap enable standard

snmp-agent target-host trap-hostname huawei address 10.10.1.10 trap-paramsname ABC
snmp-agent target-host trap-paramsname ABC v3 securityname user1 privacy
```


Copyright © Huawei Technologies Co., Ltd.

```
snmp-agent trap source meth 0

save
```

1.4.1.3 Commissioning Inband Management (SNMP V1 and V2)

This topic describes how to implement the inband network management on the MA5600T/MA5603T/MA5608T through the upstream port (inband network management port). This enables the U2000 to maintain the MA5600T/MA5603T/MA5608T through this management channel. In the inband network management mode, the service channel of the device is used to transmit the management information. The network is flexible and requires no additional devices, which helps save the cost for carriers. This network, however, is difficult to maintain.

Service Requirements

In the network as shown in **Figure 1-60**, the service requirements are as follows:

- The MA5600T/MA5603T/MA5608T provides the inband network management through the upstream port.
- The upstream port of the GIU board on the MA5600T/MA5603T/MA5608T is used as the inband network management port.
- A static route is used between the MA5600T/MA5603T/MA5608T and the U2000.

Figure 1-60 Example network for the inband network management

=

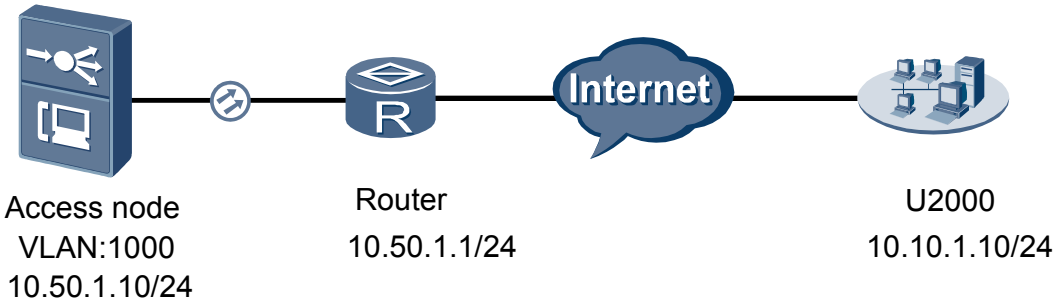
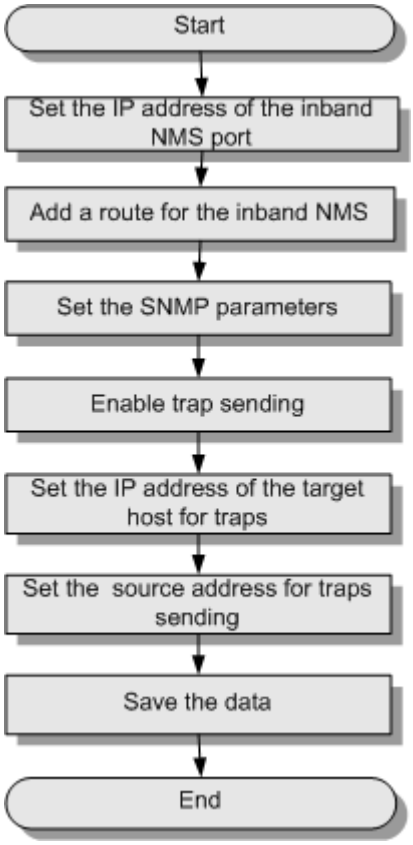


Figure 1-61 shows the flowchart for commissioning the inband network management.

Copyright © Huawei Technologies Co., Ltd.

Figure 1-61 Flowchart for commissioning the inband network management



Procedure

- Commission the inband network management on the device.
  1. Configure the IP address of the inband network management port.

     The upstream port (inband network management port) is 0/19/0, the VLAN ID is 1000, the VLAN type is standard VLAN, and the IP address is 10.50.1.10/24.

     ```
     huawei(config)#vlan 1000 standard
     huawei(config)#port vlan 1000 0/19 0
     huawei(config)#interface vlanif 1000
     huawei(config-if-vlanif1000)#ip address 10.50.1.10 255.255.255.0
     huawei(config-if-vlanif1000)#quit
     ```

     NOTE

     If the packet transmitted from the upstream port is untagged, run the **native-vlan** command to configure the native VLAN of the upstream port to be the same as the VLAN of the upstream port.

  2. Add a route for the inband network management.

     Use the static route. The destination IP address is 10.10.1.0/24 (the network segment to which the U2000 belongs), and the gateway IP address is 10.50.1.1/24 (the IP address of the gateway of the MA5600T/MA5603T/MA5608T).

     ```
     huawei(config)#ip route-static 10.10.1.0 24 10.50.1.1
     ```

  3. Set the SNMP parameters.

Copyright © Huawei Technologies Co., Ltd.

a. Configure the community name and the access authority.

The read community name is **public**, and the write community name is **private**.

NOTE

The configurations of the read community name and the write community name must be the same as the configurations on the U2000.

```
huawei(config)#snmp-agent community read public
huawei(config)#snmp-agent community write private
```

b. (Optional) Set the ID and the contact means of the administrator.

The contact means of the administrator is **HW-075528780808**.

```
huawei(config)#snmp-agent sys-info contact HW-075528780808
```

c. (Optional) Set the location of the device.

The location of the device is **Shenzhen_China**.

```
huawei(config)#snmp-agent sys-info location Shenzhen_China
```

d. Set the SNMP version.

- The SNMP version is SNMP V1.

```
huawei(config)#snmp-agent sys-info version v1
```

- The SNMP version is SNMP V2.

```
huawei(config)#snmp-agent sys-info version v2c
```

NOTE

The SNMP version must be the same as the SNMP version set on the U2000.

4. Enable the function of sending traps.

On the MA5600T/MA5603T/MA5608T, enable the function of sending traps to the U2000.

```
huawei(config)#snmp-agent trap enable standard
```

5. Configure the IP address of the destination host for the traps.

- When the SNMP V1 is used, the host name is **huawei**, the IP address of the host is **10.10.1.10/24** (IP address of the U2000), the trap parameter name is **ABC**, SNMP version is **V1**, and the parameter security name is **private** (the parameter security name is the SNMP community name).

```
huawei(config)#snmp-agent target-host trap-hostname huawei address
10.10.1.10
 trap-paramsname ABC
huawei(config)#snmp-agent target-host trap-paramsname
 ABC v1 securityname private
```

- When the SNMP V2 is used, the host name is **huawei**, the IP address of the host is **10.10.1.10/24** (IP address of the U2000), the trap parameter name is **ABC**, SNMP version is **V2**, and the parameter security name is **private** (the parameter security name is the SNMP community name).

```
huawei(config)#snmp-agent target-host trap-hostname huawei address
 10.10.1.10 trap-paramsname ABC
huawei(config)#snmp-agent target-host trap-paramsname ABC
 v2c securityname private
```

6. Configure the IP address of the VLAN interface as the source address for sending traps.

Enable the forwarding of the SNMP packets from the L3 interface of VLAN 1000 of the MA5600T/MA5603T/MA5608T.

Copyright © Huawei Technologies Co., Ltd.

```
huawei(config)#snmp-agent trap source vlanif 1000
```

7. Save the data.

```
huawei(config)#save
```

- Commission the inband network management on the U2000.

1. Configure the gateway of the route from the U2000 to network segment 10.50.1.0/24 to 10.10.1.1.
   - In the Solaris OS, do as follows:

     Run the **route add 10.50.1.0 10.10.1.1** command to add a route.

     Run the **netstat -r** command to query the information about the current routing table.
   - In the Windows OS, do as follows:

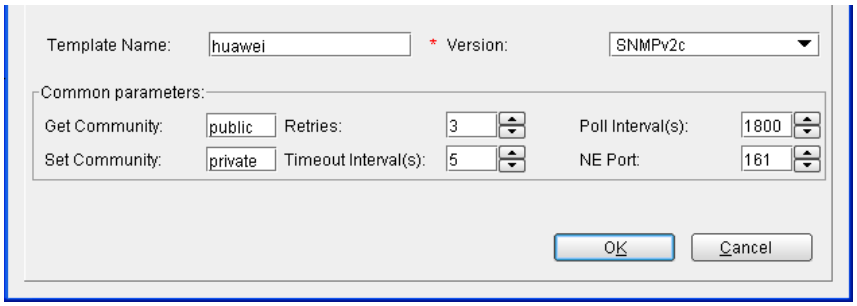
     Run the **route add 10.50.1.0 mask 255.255.255.0 10.10.1.1** command to add a route.

     Run the **route print** command to query the information about the current routing table.

   NOTE

   If the IP address of the outband network management port and the IP address of the U2000 are in the same network segment, you need not configure the routing information.
2. Log in to the U2000.
3. Set the SNMP parameters. A default SNMP profile exists in the system. Use the default profile in this service. If a new profile is required, do as follows:
   a. Choose **Administration** > **NE Communicate Parameter** > **Default Access Protocol Parameters** from the main menu.
   b. - When the SNMP V1 is used, choose **SNMP v1 Parameter** on the **Default Access Protocol Parameters** tab page. Then click **Add** and set the SNMP parameters, as shown in the following figure (the other parameters except **Profile name** use the default settings).

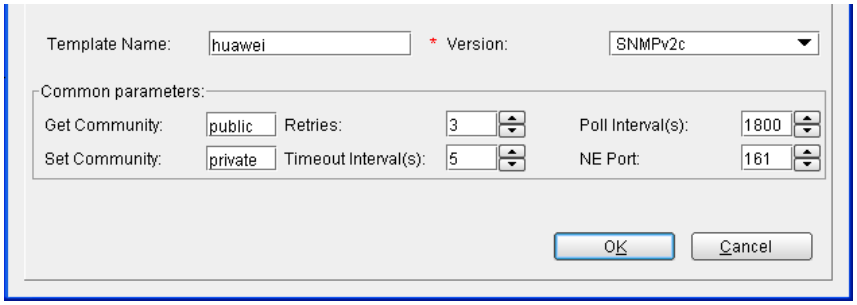
      Figure 1-62 Set the SNMP parameters

      - When the SNMP V2 is used, choose **SNMP v2 Parameter** on the **Default Access Protocol Parameters** tab page. Then click **Add** and set the SNMP parameters, as shown in the following figure (the other parameters except **Profile name** use the default settings).

Copyright © Huawei Technologies Co., Ltd.

Figure 1-63 Set the SNMP parameters



NOTE

The configurations of **Get Community** and **Set Community** are the same as the configurations on the MA5600T/MA5603T/MA5608T.

c. Click **OK**.

d. Select the added SNMP parameters. Click **OK**.

e. In the dialog box that is displayed, click **Yes** to test the set SNMP parameters.

f. The U2000 displays the **Loading** dialog box. After the testing is complete, click **OK**.

4. Add a device.

a. In the **Physical Root** navigation tree on the **Main Topology** tab page, right-click and choose **New** > **NE** from the shortcut menu.

b. In the dialog box that is displayed, choose **Access NE** > **Access NE** from the main menu.

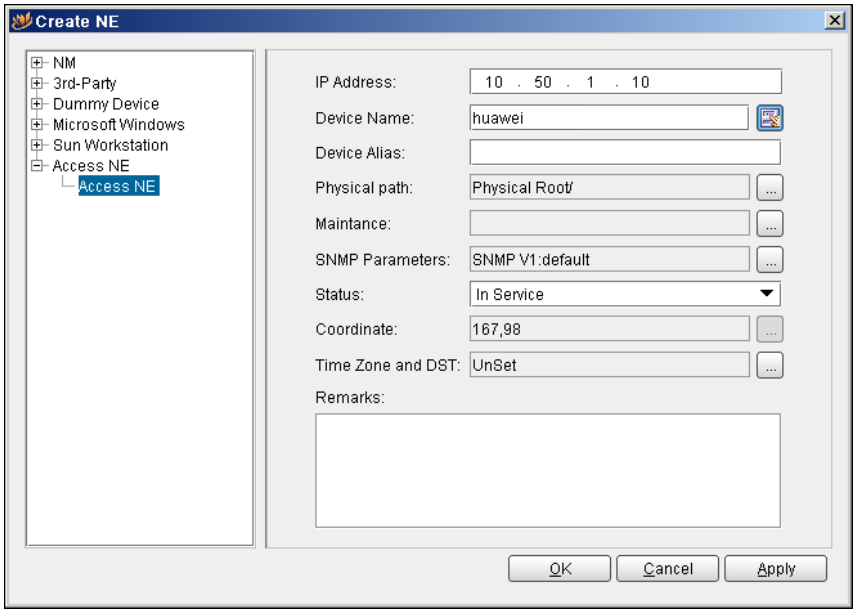
c. In the right pane, set the parameters.

- When the SNMP V1 is used, In the dialog box that is displayed, set the required parameters, as shown in the following figure.

  IP Address is **10.50.1.10**, **Device Name** is **huawei**, and **SNMP Parameters** is **SNMP V1:default**.

Copyright © Huawei Technologies Co., Ltd.

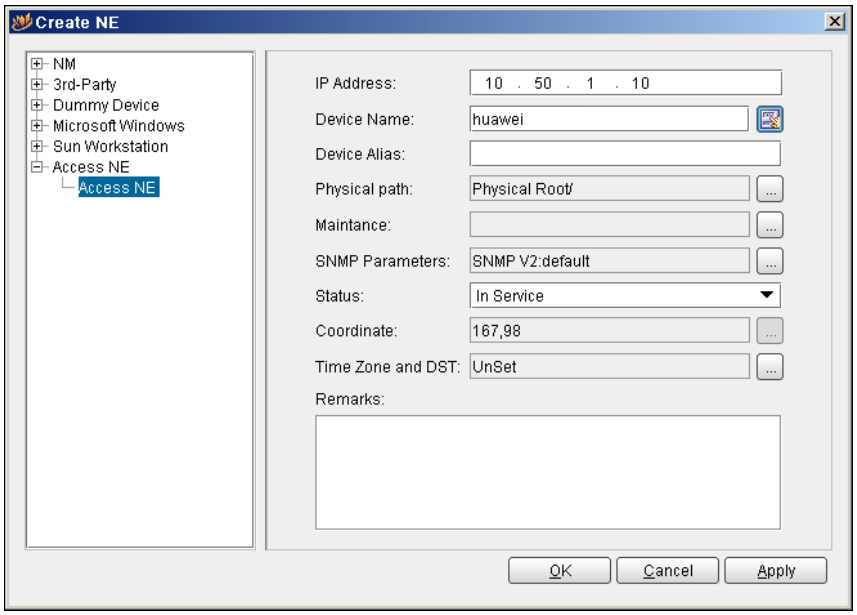
Figure 1-64 Add device



- When the SNMP V2 is used, In the dialog box that is displayed, set the required parameters, as shown in the following figure.

  IP Address is **10.50.1.10**, **Device Name** is **huawei**, and **SNMP Parameters** is **SNMP V2:default**.

Figure 1-65 Add device



Copyright © Huawei Technologies Co., Ltd.

d. Click **OK**. The system displays a message indicating that several seconds or some 10 minutes are required for uploading the device data. After the related data is read, the system automatically refreshes and displays the device icon.

----End

Result

You can maintain and manage the MA5600T/MA5603T/MA5608T through the U2000.

Configuration File

The following describes the script for commissioning the inband network management on the device (SNMP V1).

```
vlan 1000 standard
port vlan 1000 0/19 0
interface vlanif 1000
ip address 10.50.1.10 255.255.255.0

quit
ip route-static 10.10.1.0 24 10.50.1.1

snmp-agent community read public

snmp-agent community write private

snmp-agent sys-info contact HW-075528780808
snmp-agent sys-info location Shenzhen_China
snmp-agent sys-info version v1

snmp-agent trap enable standard
snmp-agent target-host trap-hostname huawei address 10.10.1.10 trap-paramsname ABC
snmp-agent target-host trap-paramsname ABC v1 securityname private

snmp-agent trap source vlanif 1000
save
```

The following describes the script for commissioning the inband network management on the device (SNMP V2).

```
vlan 1000 standard
port vlan 1000 0/19 0
interface vlanif 1000
ip address 10.50.1.10 255.255.255.0

quit
ip route-static 10.10.1.0 24 10.50.1.1

snmp-agent community read public

snmp-agent community write private

snmp-agent sys-info contact HW-075528780808
snmp-agent sys-info location Shenzhen_China
snmp-agent sys-info version v2c

snmp-agent trap enable standard
snmp-agent target-host trap-hostname huawei address 10.10.1.10 trap-paramsname ABC
snmp-agent target-host trap-paramsname ABC v2c securityname private

snmp-agent trap source vlanif 1000
save
```


Copyright © Huawei Technologies Co., Ltd.

1.4.1.4 Commissioning Inband Network Management (SNMP V3)

This topic describes how to implement the inband network management on the MA5600T/MA5603T/MA5608T through the upstream port (inband network management port). This enables the U2000 to maintain the MA5600T/MA5603T/MA5608T through this management channel. In the inband network management mode, the service channel of the device is used to transmit the management information. The network is flexible and requires no additional devices, which helps save the cost for carriers. This network, however, is difficult to maintain.

Service Requirements

In the network as shown in **Figure 1-66**, the service requirements are as follows:

- The MA5600T/MA5603T/MA5608T provides the inband network management through the upstream port.
- The upstream port of the GIU board on the MA5600T/MA5603T/MA5608T is used as the inband network management port.
- A static route is used between the MA5600T/MA5603T/MA5608T and the U2000.
- SNMP V3 is used (more reliable than V1 and V2, providing network security and access control management functions).

Figure 1-66 Example network for the inband network management

=

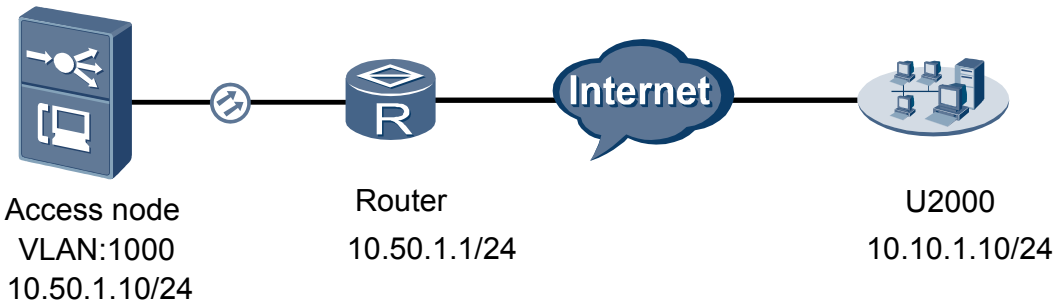
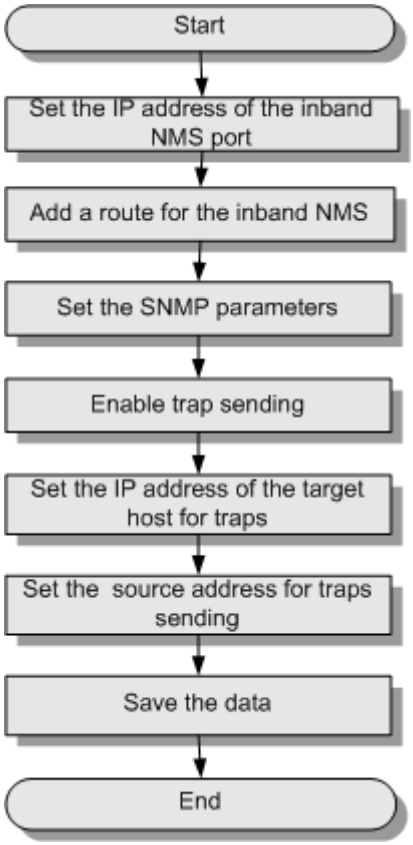


Figure 1-67 shows the flowchart for commissioning the inband network management.

Copyright © Huawei Technologies Co., Ltd.

Figure 1-67 Flowchart for commissioning the inband network management



Procedure

- Commission the inband network management on the device.
  1. Configure the IP address of the inband network management port.

     The upstream port (inband network management port) is 0/19/0, the VLAN ID is 1000, the VLAN type is standard VLAN, and the IP address is 10.50.1.10/24.

     ```
     huawei(config)#vlan 1000 standard
     huawei(config)#port vlan 1000 0/19 0
     huawei(config)#interface vlanif 1000
     huawei(config-if-vlanif1000)#ip address 10.50.1.10 255.255.255.0
     huawei(config-if-vlanif1000)#quit
     ```

     NOTE

     If the packet transmitted from the upstream port is untagged, run the **native-vlan** command to configure the native VLAN of the upstream port to be the same as the VLAN of the upstream port.
  2. Add a route for the inband network management.

     Use the static route. The destination IP address is 10.10.1.0/24 (the network segment to which the U2000 belongs), and the gateway IP address is 10.50.1.1/24 (the IP address of the gateway of the MA5600T/MA5603T/MA5608T).

     ```
     huawei(config)#ip route-static 10.10.1.0 24 10.50.1.1
     ```
  3. Log in to the U2000.
  4. Set the SNMP parameters.

Copyright © Huawei Technologies Co., Ltd.

a. Configure the SNMP user, group, and view.

The user name is **user1**, the group name is **group1**, the user authentication mode is **SHA**, the authentication password is **authkey123**, the user encryption mode is **aes128**, the encryption password is **prikey123**, the read and write view names are **hardy**, and the view includes the internet subtree.

```
huawei(config)#snmp-agent usm-user v3 user1 group1
authentication-mode sha authkey123 privacy-mode aes128 prikey123
huawei(config)#snmp-agent group v3 group1 privacy read-view hardy
write-view hardy
huawei(config)#snmp-agent mib-view hardy include internet
```

NOTE

AES128 is recommended because it has higher security than DES56.

b. (Optional) Set the ID and contact means of the administrator.

The contact means of the administrator is **HW-075528780808**.

```
huawei(config)#snmp-agent sys-info contact HW-075528780808
```

c. (Optional) Set the location of the device.

The location of the device is **Shenzhen_China**.

```
huawei(config)#snmp-agent sys-info location Shenzhen_China
```

d. (Optional) Configure the engine ID of the SNMP entity.

The engine ID of the SNMP entity is set to 0123456789.

NOTE

The context engine ID of the SNMP must be the same as that on the U2000.

```
huawei(config)#snmp-agent local-engineid 0123456789
```

e. Set the SNMP version.

The SNMP version is SNMP V3.

NOTE

The SNMP version must be the same as the SNMP version set on the U2000.

```
huawei(config)#snmp-agent sys-info version v3
```

5. Enable the function of sending traps.

On the MA5600T/MA5603T/MA5608T, enable the function of sending traps to the U2000.

```
huawei(config)#snmp-agent trap enable standard
```

6. Configure the IP address of the destination host for the traps.

The host name is **huawei**, the IP address of the host is **10.10.1.10/24** (IP address of the U2000), the trap parameter name is **ABC**, the SNMP version is **V3**, the parameter security name is **user1** (when the SNMP V3 is used, the parameter security name is the USM user name), and the traps are authenticated and encrypted.

```
huawei(config)#snmp-agent target-host trap-hostname huawei
address 10.10.1.10 trap-paramsname ABC
huawei(config)#snmp-agent target-host trap-paramsname
ABC v3 securityname user1 privacy
```

7. Configure the IP address of the VLAN interface as the source address for sending traps.

Enable the forwarding of the SNMP packets from the L3 interface of VLAN 1000 of the MA5600T/MA5603T/MA5608T.

```
huawei(config)#snmp-agent trap source vlanif 1000
```

8. Save the data.

Copyright © Huawei Technologies Co., Ltd.

```
huawei(config)#save
```

- Commission the inband network management on the U2000.
  1. Configure the gateway of the route from the U2000 server to network segment 10.50.1.0/24 to 10.10.1.1.
     - In the Solaris OS, do as follows:

       Run the **route add 10.50.1.0 10.10.1.1** command to add a route.

       Run the **netstat -r** command to query the information about the current routing table.
     - In the Windows OS, do as follows:

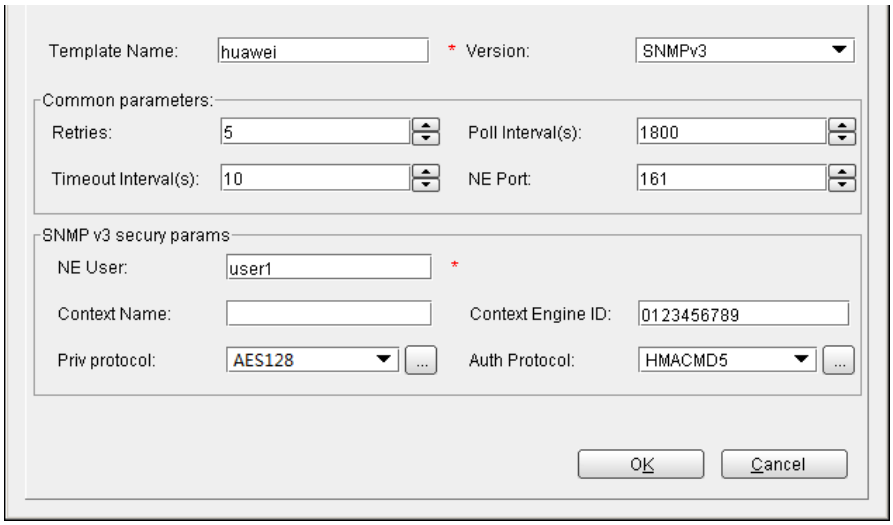
       Run the **route add 10.50.1.0 mask 255.255.255.0 10.10.1.1** command to add a route.

       Run the **route print** command to query the information about the current routing table.

     NOTE

     When the IP address of the network management port and the IP address of the U2000 are in the same network segment, you need not configure the routing information.
  2. Set the SNMP parameters.
     a. Choose **Administration** > **NE Communicate Parameter** > **Default Access Protocol Parameters** from the main menu.
     b. Choose **SNMP v3 Parameter** on the **Default Access Protocol Parameters** tab page. Then click **Add** and set the SNMP parameters, as shown in **Figure 1-68**.

     Figure 1-68 Set the SNMP parameters



     After selecting corresponding protocols in **Priv Protocol** and **Auth Protocol**, click ... next to the parameter, and set the passwords of data encryption protocol and authentication protocol, as shown in **Figure 1-69**.

Copyright © Huawei Technologies Co., Ltd.

Figure 1-69 Set the password

NOTE

NE User, **Context Engine ID**, **Priv Protocol** and password, and **Auth Protocol** and password must be the same as those configured on the MA5600T/MA5603T/MA5608T. You can run the **display snmp-agent usm-user** command to query the device user, data encryption protocol, and authentication protocol on the MA5600T/MA5603T/MA5608T and run the **display snmp-agent local-engineid** command to query the context engine ID on the MA5600T/MA5603T/MA5608T.

c. Click **OK**.

d. Select the added SNMP parameters. Click **OK**.

e. In the dialog box that is displayed, click **Yes** to test the set SNMP parameters.

f. The U2000 displays the **Loading** dialog box. After the testing is complete, click **OK**.

3. Add a device.

a. In the **Physical Root** navigation tree on the **Main Topology** tab page, right-click and choose **New** > **NE** from the shortcut menu.

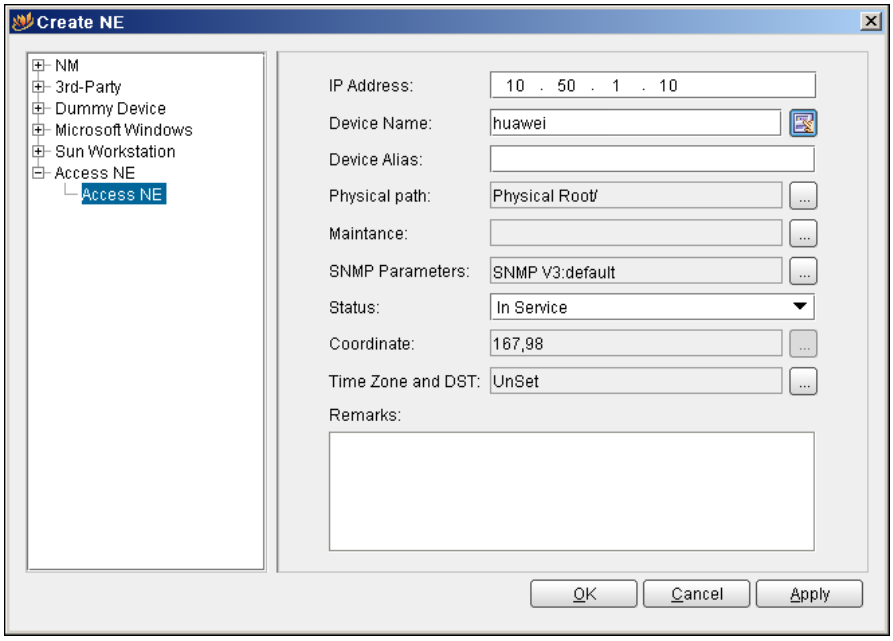
b. In the dialog box that is displayed, choose **Access NE** > **Access NE** from the main menu.

c. In the dialog box that is displayed, set the required parameters, as shown in **Figure 1-70**.

IP address is **10.50.1.10**, **Device Name** is **huawei**, **SNMP Parameters** is **SNMP V3:default**.

Copyright © Huawei Technologies Co., Ltd.

Figure 1-70 Add device



4. Click **OK**. The system prompts a message indicating that several seconds or some 10 minutes are required for uploading the device data. After the related data is read, the system automatically refreshes and displays the device icon.

----End

Result

You can maintain and manage the MA5600T/MA5603T/MA5608T through the U2000.

Configuration File

The following describes the script for commissioning the inband network management on the device.

```
vlan 1000 standard
port vlan 1000 0/19 0
interface vlanif 1000
ip address 10.50.1.10 255.255.255.0

quit
ip route-static 10.10.1.0 24 10.50.1.1

snmp-agent usm-user v3 user1 group1 authentication-mode sha authkey123 privacy-mode
aes128 prikey123
snmp-agent group v3 group1 privacy read-view hardy write-view hardy

snmp-agent mib-view hardy include internet

snmp-agent sys-info contact HW-075528780808
snmp-agent sys-info location Shenzhen_China
snmp-agent sys-info version v3

snmp-agent trap enable standard
```


Copyright © Huawei Technologies Co., Ltd.

```
snmp-agent target-host trap-hostname huawei address 10.10.1.10 trap-paramsname ABC
snmp-agent target-host trap-paramsname ABC v3 securityname user1 privacy

snmp-agent trap source vlanif 1000
save
```

1.4.2 Commissioning the Interconnection with the Router

This topic describes how to check whether the MA5600T/MA5603T/MA5608T can normally communicate with the router and whether the MA5600T/MA5603T/MA5608T can access the upper-layer device through the router.

Service Requirements

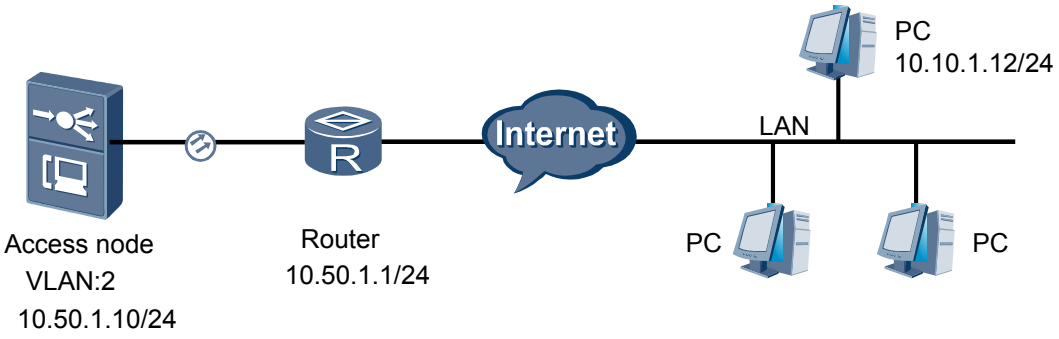
In the network as shown in **Figure 1-71**, the service requirements are as follows:

- The MA5600T/MA5603T/MA5608T uses the GIU board for upstream transmission.
- By interconnecting with the router, the MA5600T/MA5603T/MA5608T can be interconnected with the upper-layer device through configuring a static route on the MA5600T/MA5603T/MA5608T.

NOTE

For details about how to configure a router, see the related configuration guide.

Figure 1-71 Example network for commissioning the interconnection with the router



Procedure

Step 1 Configure a VLAN.

The VLAN ID is 2, and the VLAN type is smart VLAN.

```
huawei(config)#vlan 2 smart
```

Step 2 Add an upstream port to the VLAN.

Upstream port 0/19/0 is added to VLAN 2.

```
huawei(config)#port vlan 2 0/19 0
```

NOTE

If the packet transmitted from the upstream port is untagged, run the **native-vlan** command to configure the native VLAN of the upstream port to be the same as the VLAN of the upstream port.

Step 3 Configure the IP address of the L3 interface.

Copyright © Huawei Technologies Co., Ltd.

The L3 interface IP address is 10.50.1.10/24, and this IP address must be in the same network segment as the gateway IP address (IP address of the router port that is connected to the MA5600T/MA5603T/MA5608T).

```
huawei(config)#interface vlanif 2
huawei(config-if-vlanif2)#ip address 10.50.1.10 255.255.255.0
huawei(config-if-vlanif2)#quit
```

Step 4 Add a static route.

The destination IP address is 10.10.1.0/24, and the next-hop IP address is gateway IP address 10.50.1.1.

```
huawei(config)#ip route-static 10.10.1.0 24 10.50.1.1
```

Step 5 Save the data.

```
huawei(config)#save
```

----End

Result

After the MA5600T/MA5603T/MA5608T is interconnected with the router successfully, you can ping IP address 10.10.1.12 from the MA5600T/MA5603T/MA5608T.

Configuration File

```
vlan 2 smart
port vlan 2 0/19 0
interface vlanif 2
ip address 10.50.1.10 255.255.255.0

quit
ip route-static 10.10.1.0 24 10.50.1.1

save
```

1.4.3 Commissioning the Interconnection with the BRAS

This topic describes how to check whether the MA5600T/MA5603T/MA5608T can normally communicate with the BRAS. Working with the BRAS, the MA5600T/MA5603T/MA5608T can implement the authentication, accounting, and authorization (AAA) service.

Service Requirements

In the network as shown in **Figure 1-72**, the service requirements are as follows:

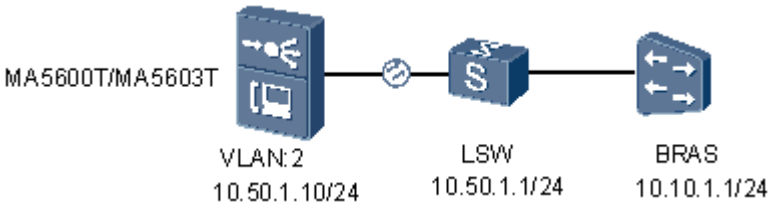
- The MA5600T/MA5603T/MA5608T uses the GIU board for upstream transmission.
- A static route is configured on the MA5600T/MA5603T/MA5608T for communicating with the BRAS.
- The requirements on the BRAS are as follows:
  - According to the authentication and accounting requirements for the users, you need to perform related configurations on the BRAS. For example, configure the access user domain (including the authentication scheme, accounting scheme, and authorization scheme that are bound to the domain) and specify the RADIUS server.
  - If the BRAS is used to authenticate users, you need to configure the user name and the password for each user on the BRAS. If the BRAS is used to allocate IP addresses, you must configure the corresponding IP address pool on the BRAS.

Copyright © Huawei Technologies Co., Ltd.

NOTE

For details about how to configure a LAN switch or the BRAS, see related configuration guides.

Figure 1-72 Example network for commissioning the interconnection with the BRAS



Procedure

Step 1 Configure a VLAN.

The VLAN ID is 2, and the VLAN type is smart VLAN.

```
huawei(config)#vlan 2 smart
```

Step 2 Add an upstream port to the VLAN.

Upstream port 0/19/0 is added to VLAN 2.

```
huawei(config)#port vlan 2 0/19 0
```

NOTE

If the packet transmitted from the upstream port is untagged, run the **native-vlan** command to configure the native VLAN of the upstream port to be the same as the VLAN of the upstream port.

Step 3 Configure the IP address of the L3 interface.

The L3 interface IP address is 10.50.1.10/24, and this IP address must be in the same network segment as the gateway IP address (IP address of the router port that is connected to the MA5600T/MA5603T/MA5608T).

```
huawei(config)#interface vlanif 2
huawei(config-if-vlanif2)#ip address 10.50.1.10 255.255.255.0
huawei(config-if-vlanif2)#quit
```

Step 4 Add a static route.

The destination IP address is 10.10.1.0/24 (the network segment of the BRAS), and the next-hop IP address is gateway IP address 10.50.1.1.

```
huawei(config)#ip route-static 10.10.1.0 24 10.50.1.1
```

Step 5 Save the data.

```
huawei(config)#save
```

----End

Result

After the MA5600T/MA5603T/MA5608T is interconnected with the BRAS successfully, you can ping IP address 10.10.1.1 from the MA5600T/MA5603T/MA5608T. After services are configured on the MA5600T/MA5603T/MA5608T, the authentication and accounting functions of the BRAS can be implemented.

Copyright © Huawei Technologies Co., Ltd.

Configuration File

```
vlan 2 smart
port vlan 2 0/19 0
interface vlanif 2
ip address 10.50.1.10 255.255.255.0

quit
ip route-static 10.10.1.0 24 10.50.1.1

save
```

1.4.4 Interconnection Commissioning of the MG Interface

The MG interface is a communication interface between the MA5600T/MA5603T/MA5608T and the MGC. Based on different control protocols between the MA5600T/MA5603T/MA5608T and the MGC, the MG interface can adopt the H.248 protocol or the MGCP protocol. The communication between the MA5600T/MA5603T/MA5608T and the MGC can be in the normal state and the services and functions can be implemented, only when the MG interface is in the normal state. This topic describes how to commission the interconnection between the MA5600T/MA5603T/MA5608T and the MGC.

1.4.4.1 Commissioning the Interconnection with the MG Interface(H.248)

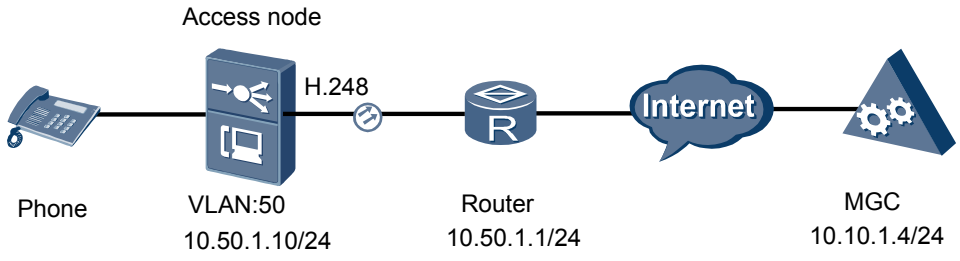
This topic describes how to check whether the MG interface can normally communicate with the MGC through the H.248 protocol.

Service Requirements

In the network as shown in **Figure 1-73**, the service requirements are as follows:

- The MA5600T/MA5603T/MA5608T uses the H.248 protocol.
- The media IP address is the same as the signaling IP address, and the media stream and the signaling stream are transmitted upstream through the same Ethernet port on the GIU board.
- The media stream and the signaling stream use the default QoS policy for upstream transmission.
- Various terminals connected to the MG interface use the default TID profile, and the software parameters of the MG interface use the default settings.
- The MGC identifies the MG through the signaling IP address (IP address of the MG interface), and their communication packets do not contain any VLAN tag.

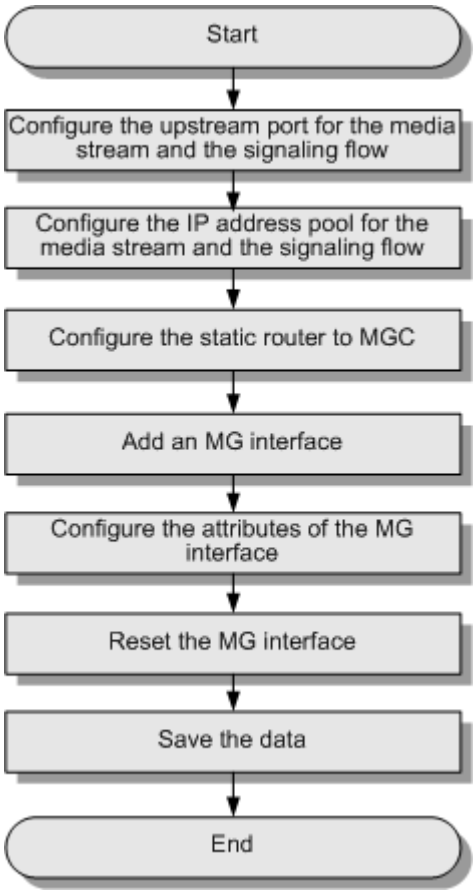
Figure 1-73 Example network for commissioning the interconnection with the MG interface (H.248)



Copyright © Huawei Technologies Co., Ltd.

Figure 1-74 shows the flowchart for commissioning the interconnection with the MG interface (H.248).

Figure 1-74 Flowchart for commissioning the interconnection with the MG interface(H.248)



Prerequisites

- The data configuration on the MGC side (corresponding to the data configuration on the MG side) must be correct.
- The current system must use the H.248 protocol.

  NOTE

  Run the **display protocol support** command to query the current voice protocol. If the voice protocol is not H.248, run the **protocol support** *h248* command to change it to H.248.

Procedure

Step 1 Configure the upstream VLAN interface for the media stream and the signaling stream.

The VLAN ID is 50, the VLAN type is smart VLAN, the upstream port is 0/19/0, and the IP address of the VLAN interface is 10.50.1.10/24.

```
huawei(config)#vlan 50 smart
huawei(config)#port vlan 50 0/19 0
huawei(config)#interface vlanif 50
huawei(config-if-vlanif50)#ip address 10.50.1.10 24
huawei(config-if-vlanif50)#quit
```


Copyright © Huawei Technologies Co., Ltd.

NOTE

If the packet transmitted from the upstream port is untagged, run the **native-vlan** command to configure the native VLAN of the upstream port to be the same as the VLAN of the upstream port.

Step 2 Configure the media and signaling IP address pools.

The media and signaling IP addresses are 10.50.1.10/24, and the gateway IP address is 10.50.1.1.

```
huawei(config)#voip
huawei(config-voip)#ip address media 10.50.1.10 10.50.1.1
huawei(config-voip)#ip address signaling 10.50.1.10
huawei(config-voip)#quit
```

NOTE

When configuring the MG interface attributes, ensure that the media and signaling IP addresses exist in the corresponding address pools.

Step 3 Configure a static route to the MGC.

The IP address of the destination network segment of the static route to the MGC is 10.10.1.0/24, and the gateway IP address is 10.50.1.1.

```
huawei(config)#ip route-static 10.10.1.0 255.255.255.0 10.50.1.1
```

Step 4 Add an MG interface.

MG interface 0 that supports the H.248 protocol is added.

```
huawei(config)#interface h248 0
  Are you sure to add MG interface?(y/n)[n]:y
```

Step 5 Configure the attributes of the MG interface.

The media and signaling IP addresses of the MG interface are 10.50.1.10/24, the MG port ID is 2944, the coding mode is text, the transmission mode is UDP, the MG domain name is MA5600T/MA5603T/MA5608T.com, the IP address of the primary MGC is 10.10.1.4/24, the MGC port ID is 2944, and the start negotiation version of the H.248 is V2.

```
huawei(config-if-h248-0)#if-h248 attribute mgip 10.50.1.10 mgport 2944 code text
transfer udp domainName
MA5600T/MA5603T/MA5608T.com primary-mgc-ip1 10.14.1.4 primary-mgc-port 2944 mg-
media-ip1 10.50.1.10 start-negotiate-version 2
```

NOTE

The start negotiation version of the H.248 protocol for the MG interface must be the same as that on the MGC side.

Step 6 Reset the MG interface.

The MG interface is reset through cold start.

```
huawei(config-if-h248-0)#reset coldstart
  Are you sure to reset MG interface?(y/n)[n]:y
huawei(config-if-h248-0)#quit
```

Step 7 Save the data.

```
huawei(config)#save
```

----End

Result

After the MG is interconnected with the MGC successfully, you can run the **display if-h248** *all* command to confirm that the MG interface is in the normal state.

```
huawei(config)#display if-h248 all
  ------------------------------------------------------------------------
  MGID   TransMode State    MGPort MGIP/DomainName MGCPort MGCIP/DomainName
  ------------------------------------------------------------------------
```


Copyright © Huawei Technologies Co., Ltd.

```
0      UDP       Normal   2944   10.50.1.10     2944    10.10.1.4
------------------------------------------------------------------------------
```

Configuration File

```
vlan 50 smart
port vlan 50 0/19 0
interface vlanif 50
ip address 10.50.1.10 24

quit
voip
ip address media 10.50.1.10 10.50.1.1
ip address signaling 10.50.1.10
quit
ip route-static 10.10.1.0 255.255.255.0 10.50.1.1

interface h248 0
y
if-h248 attribute mgip 10.50.1.10 mgport 2944 code text transfer udp domainName
MA5600T/MA5603T/MA5608T.com primary-mgc-ip1 10.14.1.4 primary-mgc-port 2944 mg-
media-ip1 10.50.1.10 start-negotiate-version 2

reset coldstart
y
quit
save
```

1.4.4.2 Commissioning the Interconnection with the MG Interface (MGCP)

This topic describes how to check whether the MG interface can normally communicate with the MGC through the MGCP protocol.

Service Requirements

In the network as shown in **Figure 1-75**, the service requirements are as follows:

- The MA5600T/MA5603T/MA5608T uses the MGCP protocol.
- The media IP address is the same as the signaling IP address (when the MGCP protocol is used, the media IP address must be the same as the signaling IP address), and the media stream and the signaling stream use the same Ethernet port on the GIU board for upstream transmission.
- The media stream and the signaling stream use the default QoS policy for upstream transmission.
- Various terminals connected to the MG interface use the default TID profile, and the software parameters of the MG interface use the default settings.
- The MGC identifies the MG through the signaling IP address (IP address of the MG interface), and their communication packets do not contain any VLAN tag.

Copyright © Huawei Technologies Co., Ltd.

Figure 1-75 Example network for the commissioning the interconnection with the MG interface (MGCP)

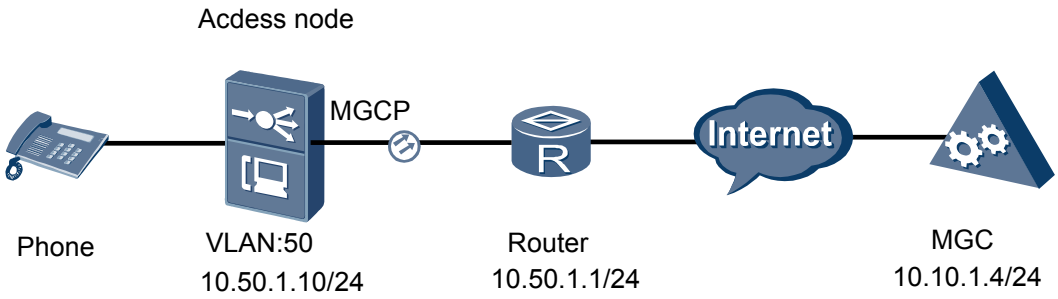
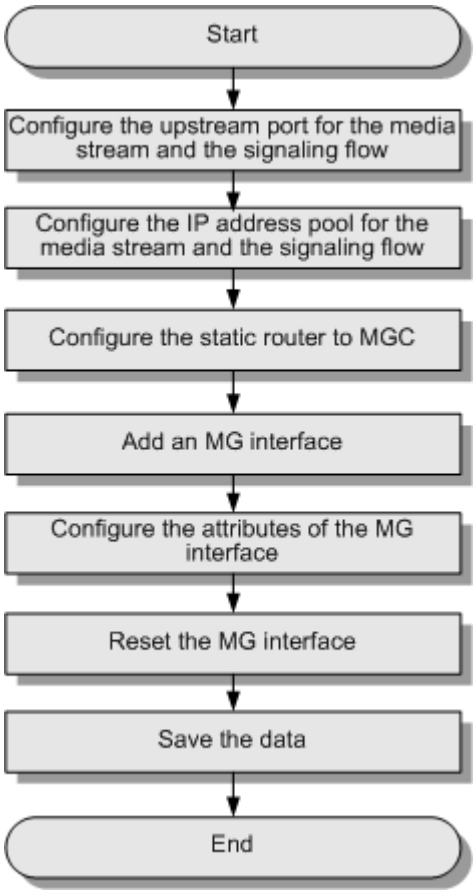


Figure 1-76 shows the flowchart for commissioning the interconnection with the MG interface (MGCP).

Figure 1-76 Flowchart for commissioning the interconnection with the MG interface (MGCP)



Prerequisites

- The data configuration on the MGC side (corresponding to the data configuration on the MG side) must be correct.

Copyright © Huawei Technologies Co., Ltd.

- The current system must use the MGCP protocol.

  NOTE

  Run the **display protocol support** command to query the current voice protocol. If the voice protocol is not MGCP, run the **protocol support** *mgcp* command to change it to MGCP.

Procedure

Step 1 Configure the upstream VLAN interface for the media stream and the signaling stream.

The VLAN ID is 50, the VLAN type is smart VLAN, and the upstream port is 0/19/0, and the IP address of the VLAN interface is 10.50.1.10/24.

```
huawei(config)#vlan 50 smart
huawei(config)#port vlan 50 0/19 0
huawei(config)#interface vlanif 50
huawei(config-if-vlanif50)#ip address 10.50.1.10 24
huawei(config-if-vlanif50)#quit
```

NOTE

If the packet transmitted from the upstream port is untagged, run the **native-vlan** command to configure the native VLAN of the upstream port to be the same as the VLAN of the upstream port.

Step 2 Configure the media and signaling IP address pools.

The media and signaling IP addresses are 10.50.1.10/24, and the gateway IP address is 10.50.1.1.

```
huawei(config)#voip
huawei(config-voip)#ip address media 10.50.1.10 10.50.1.1
huawei(config-voip)#ip address signaling 10.50.1.10
huawei(config-voip)#quit
```

NOTE

When configuring the MG interface attributes, ensure that the media and signaling IP addresses exist in the corresponding address pools.

Step 3 Configure a static route to the MGC.

The IP address of the destination network segment of the static route to the MGC is 10.10.1.0/24, and the gateway IP address is 10.50.1.1.

```
huawei(config)#ip route-static 10.10.1.0 255.255.255.0 10.50.1.1
```

Step 4 Add an MG interface.

MG interface 0 that supports the MGCP protocol is added.

```
huawei(config)#interface mgcp 0
  Are you sure to add MG interface?(y/n)[n]:y
```

Step 5 Configure the attributes of the MG interface.

The IP addresses of the MG interface is 10.50.1.10/24, the MG port ID is 2727, the coding mode is text (default setting), the transmission mode is UDP (default setting), the MG domain name is MA5600T/MA5603T/MA5608T.com, the IP address of the primary MGC is 10.10.1.4/24, and the MGC port ID is 2727.

```
huawei(config-if-mgcp-0)#if-mgcp attribute mgip 10.50.1.10 mgport 2727 domainName
MA5600T/MA5603T/MA5608T.com mgcip_1 10.10.1.4 mgcport_1 2727
```

Step 6 Reset the MG interface.

```
huawei(config-if-mgcp-0)#reset
  Are you sure to reset MG interface?(y/n)[n]:y
huawei(config-if-mgcp-0)#quit
```

Step 7 Save the data.

Copyright © Huawei Technologies Co., Ltd.

```
huawei(config)#save
```

----End

Result

After the MG is interconnected with the MGC successfully, you can run the **display if-mgcp** *all* command to confirm that the MG interface is in the normal state.

```
huawei(config)#display if-mgcp all
  ------------------------------------------------------------------------------
  MGID     State          MGPort MGIP            MGCPort MGCIP/DomainName
  ------------------------------------------------------------------------------
  0        Normal         2727   10.50.1.10      2727    10.14.1.4
  ------------------------------------------------------------------------------
```

Configuration File

```
vlan 50 smart
port vlan 50 0/19 0
interface vlanif 50
ip address 10.50.1.10 24

quit
voip
ip address media 10.50.1.10 10.50.1.1
ip address signaling 10.50.1.10
quit
ip route-static 10.10.1.0 255.255.255.0 10.50.1.1

interface mgcp 0
y
if-mgcp attribute mgip 10.50.1.10 mgport 2727 domainName MA5600T/MA5603T/
MA5608T.com mgcip_1 10.14.1.4 mgcport_1 2727

reset
y
quit
save
```

1.4.5 Commissioning the Interconnection with the SIP Interface

This topic describes how to check whether the SIP interface can normally communicate with the IP multimedia subsystem (IMS) through the SIP protocol.

Service Requirements

In the network as shown in **Figure 1-77**, the service requirements are as follows:

- The MA5600T/MA5603T/MA5608T uses the SIP protocol.
- The media IP address is the same as the signaling IP address, and the media stream and the signaling stream are transmitted upstream through the same Ethernet port on the GIU board.
- The media stream and the signaling stream use the default QoS policy for upstream transmission.
- The IMS identifies the SIP interface through the signaling IP address (IP address of the SIP interface), and their communication packets do not contain any VLAN tag.

Copyright © Huawei Technologies Co., Ltd.

Figure 1-77 Example network for commissioning the interconnection with the SIP interface

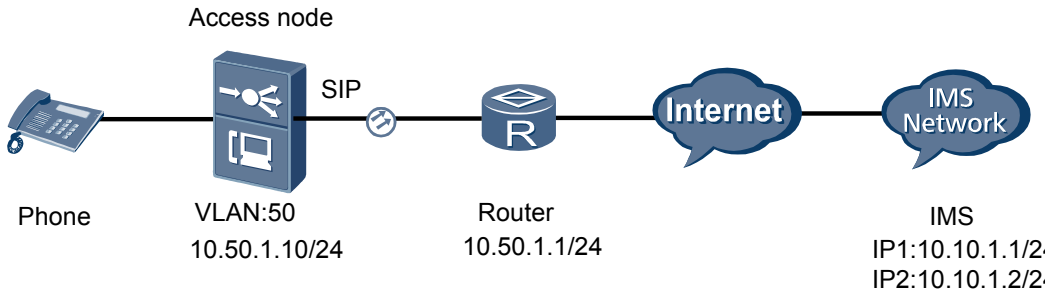
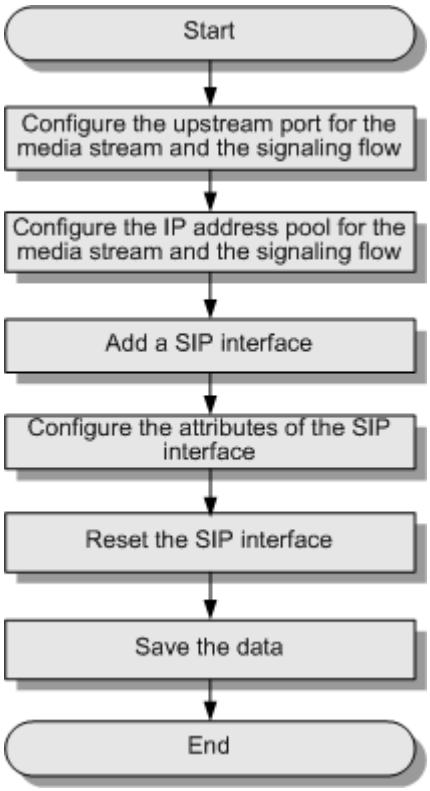


Figure 1-78 shows the flowchart for commissioning the interconnection with the SIP interface.

Figure 1-78 Flowchart for commissioning the interconnection with the SIP interface



Prerequisites

- The data configuration on the IMS side (corresponding to the data configuration on the MA5600T/MA5603T/MA5608T side) must be correct.
- The current system must use the SIP protocol.

  NOTE

  Run the **display protocol support** command to query the current voice protocol. If the voice protocol is not SIP, run the **protocol support** *sip* command to change it to SIP.

Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Configure the upstream VLAN interface for the media stream and the signaling stream.

The VLAN ID is 50, the VLAN type is smart VLAN, the upstream port is 0/19/0, and the IP address of the VLAN interface is 10.50.1.10/24.

```
huawei(config)#vlan 50 smart
huawei(config)#port vlan 50 0/19 0
huawei(config)#interface vlanif 50
huawei(config-if-vlanif50)#ip address 10.50.1.10 24
huawei(config-if-vlanif50)#quit
```

NOTE

If the packet transmitted from the upstream port is untagged, run the **native-vlan** command to configure the native VLAN of the upstream port to be the same as the VLAN of the upstream port.

Step 2 Configure the media and signaling IP address pools.

The media and signaling IP addresses are 10.50.1.10/24, and the gateway IP address is 10.50.1.1.

```
huawei(config)#voip
huawei(config-voip)#ip address media 10.50.1.10 10.50.1.1
huawei(config-voip)#ip address signaling 10.50.1.10
huawei(config-voip)#quit
```

NOTE

When configuring the SIP interface attributes, ensure that the media and signaling IP addresses exist in the corresponding address pools.

Step 3 Configure a static route to the IMS.

The IP address of the destination network segment of the static route to the IMS is 10.10.1.0/24, and the gateway IP address is 10.50.1.1.

```
huawei(config)#ip route-static 10.10.1.0 255.255.0.0 10.50.1.1
```

Step 4 Add a SIP interface.

SIP interface 0 is added.

```
huawei(config)#interface sip 0
  Are you sure to add the SIP interface?(y/n)[n]:y
```

Step 5 Configure the basic attributes of the SIP interface.

The media and signaling IP addresses of the SIP interface are 10.50.1.10/24, the signaling port ID is 5555, the transmission protocol is UDP (default setting), the IP address 1 of the primary proxy server is 10.10.1.1/24, the port ID of the primary proxy server is 5555, the IP address 1 of the secondary proxy server is 10.10.1.2/24, the port ID of the secondary proxy server is 5555, the home domain name is MA5600T/MA5603T/MA5608T.com, and the profile index is 0.

```
huawei(config-if-sip-0)#if-sip attribute basic media-ip 10.50.1.10 signal-ip
10.50.1.10 signal-port 5555 transfer udp primary-proxy-ip1 10.10.1.1 primary-proxy-
port 5555
secondary-proxy-ip1 10.10.1.2 secondary-proxy-port 5555 home-domain MA5600T/
MA5603T/MA5608T.com sipprofile-index 0
```

Step 6 Configure the optional attributes of the SIP interface.

The domain name of the SIP interface is huawei.com, and the phone context is +86755.

```
huawei(config-if-sip-0)#if-sip attribute optional mg-domain huawei.com phone-
context +86755
```

Step 7 Reset the SIP interface.

```
huawei(config-if-sip-0)#reset
  Are you sure to reset SIP interface?(y/n)[n]:y
huawei(config-if-sip-0)#quit
```


Copyright © Huawei Technologies Co., Ltd.

Step 8 Save the data.

```
huawei(config)#save
```

----End

Result

After the SIP interface is interconnected with the IMS successfully, you can run the **display if-sip** *all* command to confirm that the SIP interface is in the normal state.

```
huawei(config)#display if-sip all
  ------------------------------------------------------
  MGID     TransMode State      SignalPort SignalIP
  ------------------------------------------------------
  0        UDP       Normal     5555       10.50.1.10
  ------------------------------------------------------
```

Configuration File

```
vlan 50 smart
port vlan 50 0/19 0
interface vlanif 50
ip address 10.50.1.10 24

quit
voip
ip address media 10.50.1.10 10.50.1.1
ip address signaling 10.50.1.10
quit
ip route-static 10.10.1.0 255.255.255.0 10.50.1.1

interface sip 0
y
if-sip attribute basic media-ip 10.50.1.10 signal-ip
10.50.1.10 signal-port 5555 transfer udp primary-proxy-ip1 10.10.1.1 primary-proxy-
port 5555
secondary-proxy-ip1 10.10.1.2 secondary-proxy-port 5555 home-domain MA5600T/
MA5603T/MA5608T.com sipprofile-index 0

if-sip attribute optional mg-domain huawei.com phone-context +86755

reset
y
quit
save
```

1.4.6 Commissioning the Management Channel Between the OLT and the GPON MDU

This topic describes how to commission the management channel between the MA5600T/MA5603T/MA5608T and the GPON MDU to ensure that you can log in to the GPON MDU using the MA5600T/MA5603T/MA5608T at the CO to remotely maintain and manage the GPON MDU.

Service Requirements

In the network as shown in **Figure 1-79**, the service requirements are as follows:

- A GPON port on the MA5600T/MA5603T/MA5608T is connected to 128 MDUs using an optical splitter.

Copyright © Huawei Technologies Co., Ltd.

NOTE

The following considers MDU 0 as an example for commissioning the management channel between the OLT and the GPON MDU.

- After the management channel between the MA5600T/MA5603T/MA5608T and the GPON MDU is set up, you can log in to the MDU using port 0/2/0 connected to the MDU to remotely maintain and manage the MDU.
- The DBA profile is used to limit the user rate to the fixed 10 Mbit/s bandwidth.

Figure 1-79 Example network for commissioning the management channel between the OLT and the GPON MDU

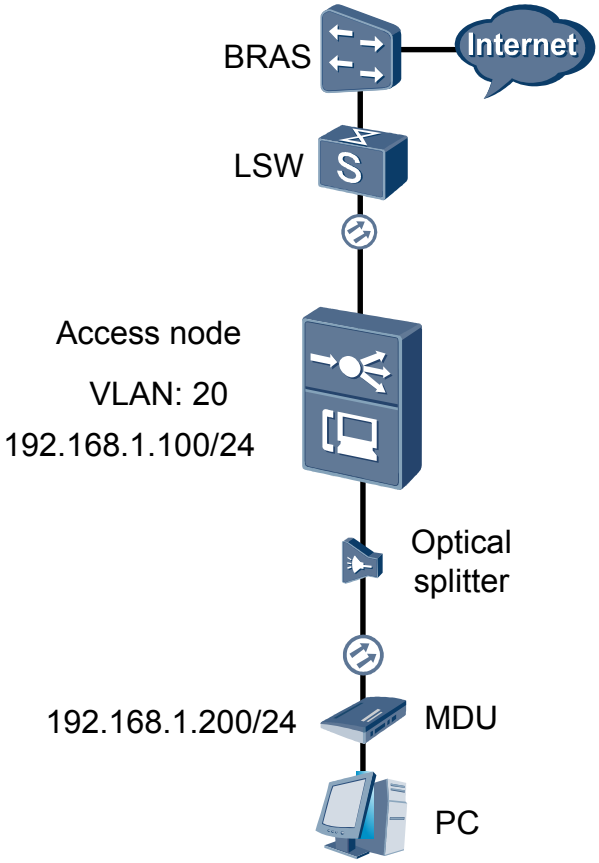
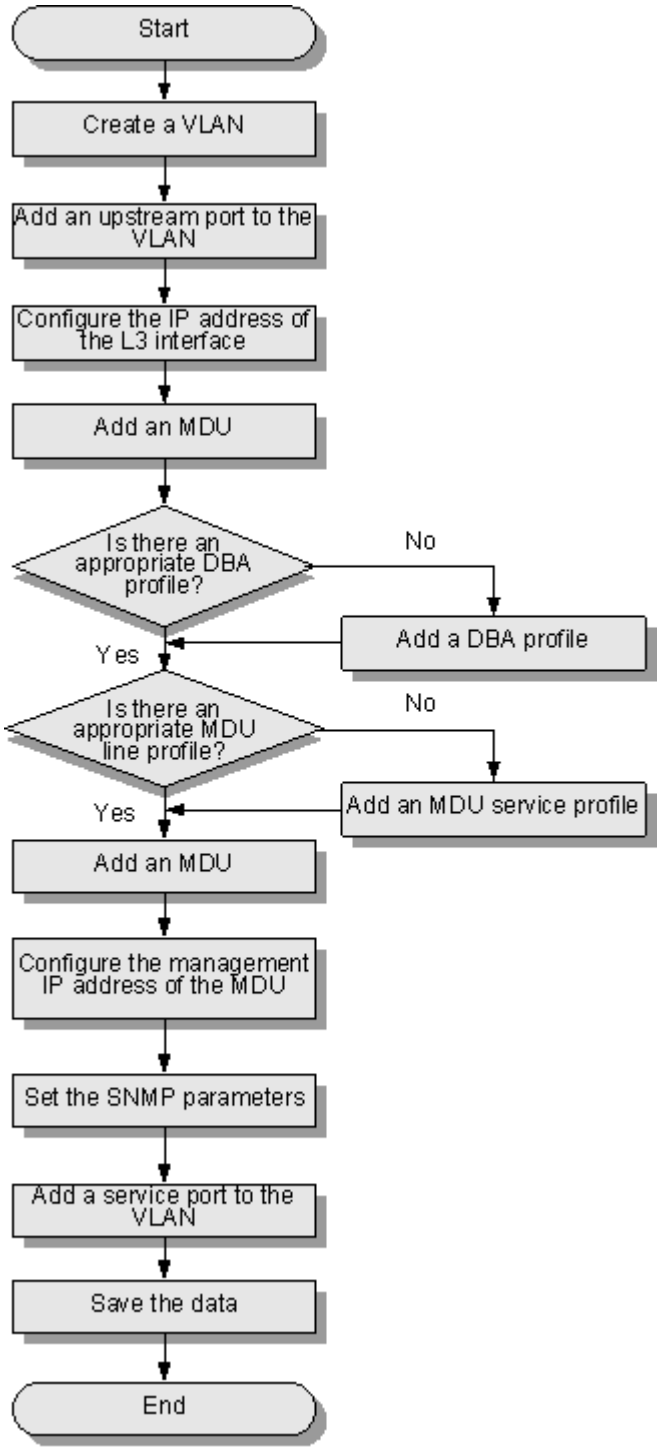


Figure 1-80 shows the flowchart for commissioning the management channel between the OLT and the GPON MDU.

Copyright © Huawei Technologies Co., Ltd.

Figure 1-80 Flowchart for commissioning the management channel between the OLT and the GPON MDU



Procedure

Step 1 Create a VLAN.

The VLAN ID is 20, and the VLAN type is smart VLAN.

Copyright © Huawei Technologies Co., Ltd.

```
huawei(config)#vlan 20 smart
```

Step 2 Add an upstream port to the VLAN.

Upstream port 0/19/0 on the GIU board is added to VLAN 20.

```
huawei(config)#port vlan 20 0/19 0
```

Step 3 Configure the IP address of the Layer 3 interface.

The Layer 3 IP address is 192.168.1.100/24.

```
huawei(config)#interface vlanif 20
huawei(config-if-vlanif20)#ip address 192.168.1.100 255.255.255.0
huawei(config-if-vlanif20)#quit
```

Step 4 Add a DBA profile.

The DBA profile ID is 12, the DBA profile uses the default name DBA-profile_12, the bandwidth type is type1 (fixed bandwidth), and the user rate is the fixed 10 Mbit/s bandwidth.

NOTE

- The bandwidth type and the attribute of the DBA profile must be compatible with the service to be carried.
- The system supports five DBA profile types, namely, type1 (fixed bandwidth), type2 (assured bandwidth), type3 (assured bandwidth+maximum bandwidth), type4 (maximum bandwidth), and type5 (fixed bandwidth+assured bandwidth+maximum bandwidth).
- By default, the system provides DBA profiles 1 to 9, each of which provides typical values for traffic parameters. By default, T-CONT 0 is bound with DBA profile 1.
- The value of the bandwidth you input when adding the DBA profile rounds down to the nearest integer multiple of 64. For example, if the input bandwidth value is 1022 kbit/s, the actual bandwidth is 960 kbit/s.
- You can run the **display dba-profile** command to query the information about the DBA profile.

```
huawei(config)#dba-profile add profile-id 12 type1 fix 10240
```

Step 5 Configure an MDU line profile.

The MDU line profile ID is 5, T-CONT 1 is bound with DBA profile 12, GEM port 0 is bound to T-CONT 1, the service type is ETH, and the mapping mode is VLAN mapping.

```
huawei(config)#ont-lineprofile gpon profile-id 5
huawei(config-gpon-lineprofile-5)#tcont 1 dba-profile-id 12
huawei(config-gpon-lineprofile-5)#gem add 0 eth tcont 1
huawei(config-gpon-lineprofile-5)#gem mapping 0 0 vlan 20
huawei(config-gpon-lineprofile-5)#commit
huawei(config-gpon-lineprofile-5)#quit
```

Step 6 Add an MDU.

MDU 0 is connected to GPON port 0, the MDU authentication mode is the SN authentication, the SN is 32303131B39FD641, the management protocol is SNMP, and MDU profile 5 is bound to MDU 0.

NOTE

You can add an MDU in the following two ways: confirming an auto-discovered MDU and adding an MDU offline. Here, the method of adding an MDU offline is considered as an example.

You can also run the **port ont-auto-find** command to enable the function of auto-discovering an MDU, and then run the **ont confirm** command to confirm the auto-discovered MDU.

```
huawei(config)#interface gpon 0/2
huawei(config-if-gpon-0/2)#ont add 0 0 sn-auth 32303131B39FD641 snmp ont-
lineprofile-id 5
```

Step 7 Configure the management IP address of the MDU.

Copyright © Huawei Technologies Co., Ltd.

The management IP address is 192.168.1.200/24, and the ID of the native VLAN to which the MDU port belongs is 20.

```
huawei(config-if-gpon-0/2)#ont ipconfig 0 0 static ip-address 192.168.1.200 mask
255.255.255.0 vlan 20
huawei(config-if-gpon-0/2)#quit
```

Step 8 Set the SNMP parameters.

Configure the SNMP profile 10. That, the SNMP version is SNMP V2C, the read community name is **public**, and the write community name is **private**, the IP address of the U2000 is **10.10.1.10/24**, the port is 162, the parameter security name is **user1** (the parameter security name is the write community name), the gateway IP address is 192.168.1.101.

```
huawei(config)#snmp-profile add profile-id 10 v2c public
private 10.10.1.10 162 private
huawei(config)#interface gpon 0/2
huawei(config-if-gpon-0/2)#ont snmp-profile 0 0 profile-id 10
huawei(config-if-gpon-0/2)#ont snmp-route 0 0 ip-address 10.10.1.10 mask
255.255.255.0 next-hop 192.168.1.101
huawei(config-if-gpon-0/2)#quit
```

Step 9 Add a service port to the VLAN.

```
huawei(config)#service-port vlan 20 gpon 0/2/0 ont 0 gemport 0 multi-service user-
vlan 20
```

Step 10 Save the data.

```
huawei(config)#save
```

----End

Result

After the commissioning is complete, you can remotely maintain and manage the MDU using **telnet 192.168.1.200**.

Configuration File

```
vlan 20 smart
port vlan 20 0/19 0
interface vlanif 20
ip address 192.168.1.100 255.255.255.0

quit
dba-profile add profile-id 12 type1 fix 10240

ont-lineprofile gpon profile-id 5

tcont 1 dba-profile-id 12
gem add 0 eth tcont 1

gem mapping 0 0 vlan 20

commit
quit
interface gpon 0/2
ont add 0 0 sn-auth 32303131B39FD641 snmp ont-lineprofile-id 5

ont ipconfig 0 0 static ip-address 192.168.1.200 mask 255.255.255.0 vlan 20

quit
snmp-profile add profile-id 10 v2c public private 10.10.1.10 162 private
interface gpon 0/2
ont snmp-profile 0 0 profile-id 10
ont snmp-route 0 0 ip-address 10.10.1.10 mask 255.255.255.0 next-hop 192.168.1.101
```


Copyright © Huawei Technologies Co., Ltd.

```
quit
service-port vlan 20 gpon 0/2/0 ont 0 gemport 0 multi-service user-vlan 20

save
```

1.4.7 Commissioning the Management Channel Between the OLT and the GPON ONT

This topic describes how to commission the GPON OLT to ensure that the service configuration and centralized management of the GPON ONTs are performed on the GPON OLT using the ONT Management and Control Interface (OMCI) protocol.

Service Requirements

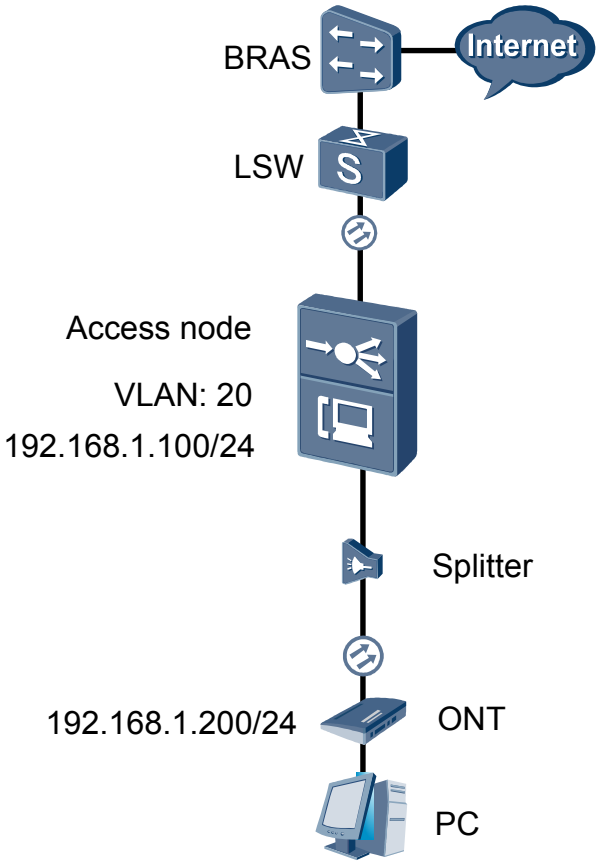
In the network as shown in **Figure 1-81**, the service requirements are as follows:

- A GPON port on the MA5600T/MA5603T/MA5608T is connected to 128 ONTs using an optical splitter.

  NOTE

  The following considers ONT 0 as an example for commissioning the management channel between the OLT and the GPON ONT.
- On the MA5600T/MA5603T/MA5608T, you can configure ONTs at different locations in a centralized manner.
- The DBA profile is used to limit the user rate to the fixed 10 Mbit/s bandwidth.

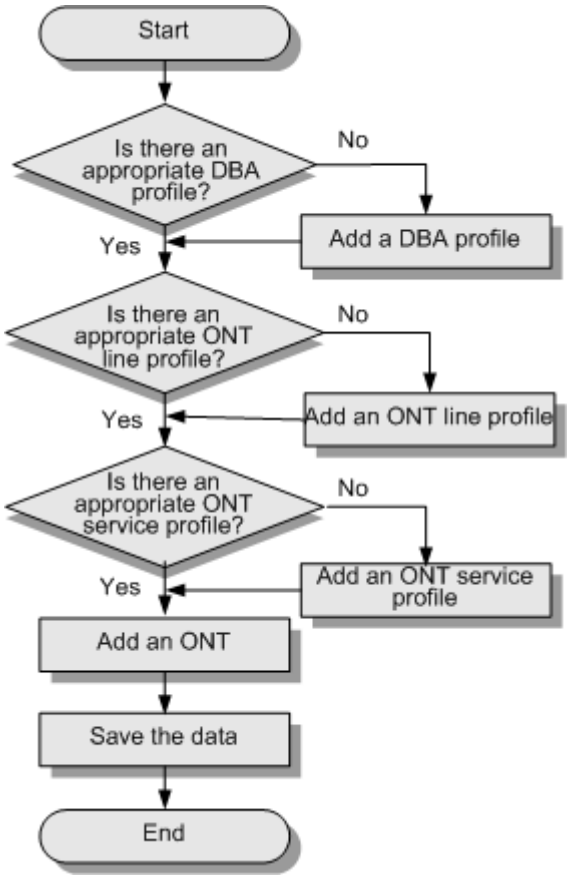
Figure 1-81 Example network for commissioning the management channel between the OLT and the GPON ONT



Copyright © Huawei Technologies Co., Ltd.

Figure 1-82 shows the flowchart for commissioning the management channel between the OLT and the GPON ONT.

Figure 1-82 Flowchart for commissioning the management channel between the OLT and the GPON ONT



Procedure

Step 1 Add a DBA profile.

The DBA profile ID is 12, the DBA profile uses the default name DBA-profile_12, the bandwidth type is type1 (fixed bandwidth), and the user rate is the fixed 10 Mbit/s bandwidth.

Copyright © Huawei Technologies Co., Ltd.

NOTE

- The bandwidth type and the attribute of the DBA profile must be compatible with the service to be carried.
- The system supports five DBA profile types, namely, type1 (fixed bandwidth), type2 (assured bandwidth), type3 (assured bandwidth+maximum bandwidth), type4 (maximum bandwidth), and type5 (fixed bandwidth+assured bandwidth+maximum bandwidth).
- By default, the system provides DBA profiles 1 to 9, each of which provides typical values for traffic parameters. By default, T-CONT 0 is bound with DBA profile 1.
- The value of the bandwidth you input when adding the DBA profile rounds down to the nearest integer multiple of 64. For example, if the input bandwidth value is 1022 kbit/s, the actual bandwidth is 960 kbit/s.
- You can run the **display dba-profile** command to query the information about the DBA profile.

```
huawei(config)#dba-profile add profile-id 12 type1 fix 10240
```

Step 2 Add an ONT line profile.

The ONT line profile ID is 5, T-CONT 1 is bound with DBA profile 12, GEM port 0 is bound to T-CONT 1, the service type is ETH, and the mapping mode is VLAN mapping.

```
huawei(config)#ont-lineprofile gpon profile-id 5
huawei(config-gpon-lineprofile-5)#tcont 1 dba-profile-id 12
huawei(config-gpon-lineprofile-5)#gem add 0 eth tcont 1
huawei(config-gpon-lineprofile-5)#gem mapping 0 0 vlan 20
huawei(config-gpon-lineprofile-5)#commit
huawei(config-gpon-lineprofile-5)#quit
```

Step 3 Add an ONT service profile.

The ONT service profile ID is 10, the quantity of Ethernet ports on the ONT is 4, the quantity of POTS ports on the ONT is 2, and Ethernet ports 1-4 are added to VLAN 20.

NOTE

The port capability set in the ONT service profile must be the same as the actual ONT capability set.

```
huawei(config)#ont-srvprofile gpon profile-id 10
huawei(config-gpon-srvprofile-10)#ont-port eth 4 pots 2
huawei(config-gpon-srvprofile-10)#port vlan eth 1-4 20
huawei(config-gpon-srvprofile-10)#commit
huawei(config-gpon-srvprofile-10)#quit
```

Step 4 Add an ONT.

ONT 0 is connected to GPON port 0, the ONT authentication mode is the SN authentication, the SN is 323031314D4B2041, the management protocol is OMCI, and ONT line profile 5 and ONT service profile 10 are bound to ONT 0.

NOTE

You can add an ONT in the following two ways: confirming an auto-discovered ONT and adding an ONT offline. Here, the method of adding an ONT offline is considered as an example.

You can also run the **port ont-auto-find** command to enable the function of auto-discovering an ONT, and then run the **ont confirm** command to confirm the auto-discovered ONT.

```
huawei(config)#interface gpon 0/2

huawei(config-if-gpon-0/2)#ont add 0 0 sn-auth 323031314D4B2041 omci ont-
lineprofile-id 5 ont-srvprofile-id 10
huawei(config-if-gpon-0/2)#quit
```

Step 5 Save the data.

```
huawei(config)#save
```

----End

Copyright © Huawei Technologies Co., Ltd.

Result

After the commissioning is complete, you can maintain and manage the ONT on the MA5600T/MA5603T/MA5608T (For example, run the **ont deactivate** command to deactivate the ONT that is in the activated state).

Configuration File

```
vlan 20 smart
port vlan 20 0/19 0
interface vlanif 20
ip address 192.168.1.100 255.255.255.0

quit
dba-profile add profile-id 12 type1 fix 10240

ont-lineprofile gpon profile-id 5

tcont 1 dba-profile-id 12
gem add 0 eth tcont 1

gem mapping 0 0 vlan 20

commit
quit
interface gpon 0/2
ont add 0 0 sn-auth 32303131B39FD641 snmp ont-lineprofile-id 5

ont ipconfig 0 0 static ip-address 192.168.1.200 mask 255.255.255.0 vlan 20

quit
service-port vlan 20 gpon 0/2/0 ont 0 gemport 0 multi-service user-vlan 20

save
```

1.4.8 Commissioning the Management Channel to the xDSL CPE

This topic describes how to commission the CPE management function of the MA5600T/MA5603T/MA5608T to ensure that you can log in to the CPE from the DSLAM at the CO to remotely maintain and manage the CPE.

Service Requirements

In the network as shown in **Figure 1-83**, the service requirements are as follows:

- The maintenance terminal is connected to the maintenance Ethernet port of the MA5600T/MA5603T/MA5608T.
- After the management channel between the DSLAM and the CPE is set up, you can log in to the CPE using port 0/2/0 connected to the CPE to remotely maintain and manage the CPE.
- The user access mode is IPoA.

Copyright © Huawei Technologies Co., Ltd.

Figure 1-83 Example network for managing the CPE

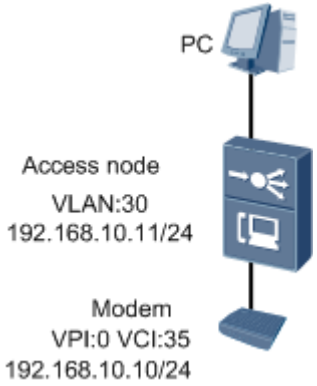
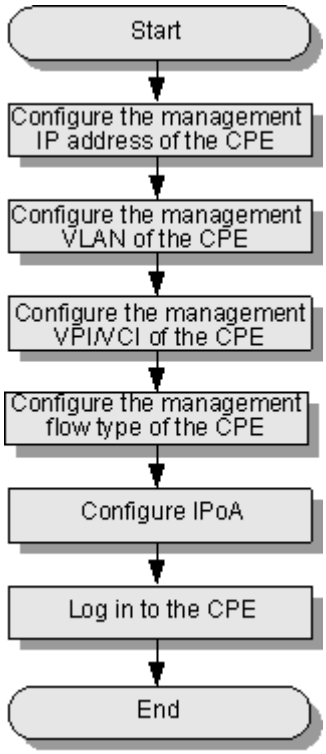


Figure 1-84 shows the flowchart for commissioning the management channel to the CPE.

Figure 1-84 Flowchart for commissioning the management channel to the CPE



Prerequisites

You must be logged in to the MA5600T/MA5603T/MA5608T using the maintenance terminal.

Procedure

Step 1 Configure the management IP address of the CPE.

Copyright © Huawei Technologies Co., Ltd.

The management IP address of the CPE is 192.168.10.10/24.

```
huawei(config)#cpe-management ip-address 192.168.10.10
```

Step 2 Configure the management VLAN of the CPE.

The VLAN ID is 30, the VLAN type is smart VLAN, and the IP address of the VLAN L3 interface is 192.168.10.11/24.

```
huawei(config)#vlan 30 smart
huawei(config)#cpe-management vlan 30
huawei(config)#interface vlanif 30
huawei(config-if-vlanif30)#ip address 192.168.10.11 24
huawei(config-if-vlanif30)#quit
```

Step 3 Configure the management VPI and VCI of the CPE.

The management VPI ID is 0, and the management VCI ID is 35.

```
huawei(config)#cpe-management vpi 0 vci 35
```

Step 4 Configure the management flow type of the CPE.

The management flow type is vlan-ethertype ipoe.

```
huawei(config)#cpe-management flow-type vlan-ethertype ipoe
```

Step 5 Configure IPoA.

Configure MAC address pool 0 with the start address 0000-0000-0001.

```
huawei(config)#mac-pool 0 0000-0000-0001
```

Enable the IPoA protocol conversion function.

```
huawei(config)#ipoa enable
```

Set the IPoA default gateway.

```
huawei(config)#ipoa default gateway 10.1.1.1
```

Step 6 Log in to the CPE.

```
huawei(config)#cpe-management telnet 0/2/0
```

----End

Result

You can log in to the CPE from the MA5600T/MA5603T/MA5608T using the maintenance terminal to maintain and manage the CPE.

Configuration File

```
cpe-management ip-address 192.168.10.10
vlan 30 smart
cpe-management vlan 30
interface vlanif 30
ip address 192.168.10.11 24
quit

cpe-management vpi 0 vci 35
cpe-management flow-type vlan-ethertype ipoe
mac-pool 0 0000-0000-0001

ipoa enable
ipoa default gateway 10.1.1.1
cpe-management telnet 0/2/0
```


Copyright © Huawei Technologies Co., Ltd.

1.5 Maintenance and Management Commissioning

To ensure the stability of the MA5600T/MA5603T/MA5608T, you need to verify the maintainability and reliability of the device after completing the stand-alone commissioning and interconnection commissioning.

1.5.1 Configuring the System Energy-Saving Function

This topic describes how to power off a board that is not configured with any services for a long time to reduce the system power and therefore to reduce the system energy consumption.

Prerequisites

NOTE

Only the MA5600T supports this operation.

The board must support the power-off mode and the energy-saving mode.

Context

Energy-saving modes include the manual energy-saving mode and automatic energy-saving mode.

- Manual energy-saving mode (powering off a board manually). You can manually power off an unused board in the subrack according to the plan for the energy-saving purpose. When the service is provisioned from the OSS server to a board that is powered off, the system prompts that the board is currently powered off. In this case, you can manually power on the board according to the prompt.
- Automatic energy-saving mode (automatically powering off a board). When the automatic energy-saving mode is enabled, the system supports a series of energy-saving measures according to the referenced energy-saving profile. These measures include the following: battery energy saving, shutting down unused boards, putting unused xDSL ports to sleep mode and shutting down the laser on unused xPON ports. An energy-saving profile is a set of energy-saving measures. The system provides three typical energy-saving profiles. You can query the profiles but cannot modify, rename, or delete them. The three typical profiles are as follows:
  - Standard energy-saving profile **standard**, with ID 1. It is the default energy-saving profile in the system. In this profile, all the energy-saving measures are disabled.
  - Basic energy-saving profile **basic**, with ID 2. In this profile, some energy-saving measures that do not affect the current services are enabled, such as:
    - Shutting down unused boards
    - Shutting down the laser on unused xPON ports and putting unused xDSL ports to sleep mode
  - Deep energy-saving profile **deep**, with ID 3. In this profile, all the energy-saving measures are enabled, and the battery energy saving may affect the service running.
- To power on a board that is powered off manually, you must run the **board power-on** command to manually power it on.

Copyright © Huawei Technologies Co., Ltd.

- You can recover the power supply of the board that is automatically powered off in the following three ways:
  - Run the **board power-on** command to power on the board.
  - Remove the board from the slot that is automatically powered off, and the system determines that the board is offline and then recovers the power supply of the slot. After the power supply is recovered, reinstall the board.
  - The system periodically (every 15 minutes) polls all boards that are automatically powered off, and determines whether the boards can be powered on. If the boards meet the power-on requirements, the system automatically powers on the boards.

Procedure

- Set the manual energy-saving mode.
  1. Run the **board power-off** command to manually power off a board.
- Set the automatic energy-saving mode.
  1. Run the spm-profile command to create an energy-saving profile. By default, the system uses the standard energy-saving profile. That is, the energy-saving mode is disabled by default. You can enable the required energy-saving measure according to actual requirements.
     - Run the battery energy-saving command to set the status of the mains monitoring module and battery energy saving.
     - Run the unused-port shutdown command to set energy saving for unused ports.
     - Run the unused-slot shutdown command to set energy saving for unused boards.
  2. Run the **system energy-saving mode** command to set the used energy-saving profile.
  3. Run the **display system energy-saving mode** command to query the used energy-saving profile.

----End

Result

The system is referenced to an energy-saving profile (that is, the unused board is shut down). If a board is not used 15 minutes after it is confirmed and functions properly, the board is powered off automatically.

Example

To reference energy-saving profile 4 to enable the system energy-saving function, do as follows: Assume that battery energy saving is enabled and energy saving for unused boards is enabled.

```
huawei(config)#spm-profile profile-id 4
huawei(config-spm-prof-4)#unused-slot shutdown enable
huawei(config-spm-prof-4)#battery energy-saving ac-monitor emuid 1 digitalid 6
huawei(config-spm-prof-4)#battery energy-saving enable
huawei(config-spm-prof-4)#quit
huawei(config)#system energy-saving mode profile-id 4
huawei(config)#display system energy-saving mode
  Current spm-profile id  : 4
  Current spm-profile name: spm_profile_4
```


Copyright © Huawei Technologies Co., Ltd.

1.5.2 Checking Alarms and Events

This topic describes how to check the alarm and event reporting function of the device.

1.5.2.1 Verifying the Alarm and Event Function

This topic describes how to verify the alarm and event function by triggering various alarms and events through the related operations.

Verifying Operation

Table 1-46 lists the operations for verifying the alarm and event function.

Table 1-46 Operations for verifying the alarm and event function

Operation	Description
Remove a service board.	Check whether the corresponding alarm or event is generated on the maintenance terminal.
Insert the service board back into the slot.	Check whether the corresponding recovery alarm or event is generated on the maintenance terminal.
Remove the optical fiber connected to an optical port.	Check whether the corresponding alarm or event is generated on the maintenance terminal.
Insert the optical fiber back into the optical port.	Check whether the corresponding recovery alarm or event is generated on the maintenance terminal.
Remove the optical fiber connected to an optical port when an ONT is online.	Check whether the corresponding alarm or event is generated on the maintenance terminal.
Insert the optical fiber back into the optical port.	Check whether the corresponding recovery alarm or event is generated on the maintenance terminal.
Open the cabinet door.	Check whether the corresponding alarm or event is generated on the maintenance terminal.
Close the cabinet door.	Check whether the corresponding recovery alarm or event is generated on the maintenance terminal.
Remove the fan tray from the shelf.	Check whether the corresponding alarm or event is generated on the maintenance terminal.
Insert the fan tray back into the shelf.	Check whether the corresponding recovery alarm or event is generated on the maintenance terminal.
Perform the active/standby switchover of the control boards.	Log in to the system, and run the **display event history** command to check whether the active/standby switchover event history exists.

1.5.2.2 Querying Alarms and Events

This topic describes how to query history alarms and events through the maintenance terminal.

Copyright © Huawei Technologies Co., Ltd.

Context

Up to 1001 latest fault alarms and recovery alarms, and 901 event alarms can be saved in the system. If the record table is full, and a new alarm or event is generated, the new alarm or event overwrites the oldest record in the record table. You can query the records that have been overwritten in the NMS database.

The CLI provides multiple ways to query history alarms and events.

Table 1-47 lists the commands for querying history alarms.

Table 1-47 Commands for querying history alarms

To...	Run the Command...
Query alarms by alarm SN	**display alarm history alarmsn** *sn* [**detail** | **list**]
Query alarms by alarm ID	**display alarm history alarmid** *id* [**detail** | **list** | **start-number** *number*]
Query alarms by alarm type	**display alarm history alarmtype** *type* [**detail** | **list** | **start-number** *number*]
Query alarms by alarm class	**display alarm history alarmclass** *class* [**detail** | **list** | **start-number** *number*]
Query alarms by alarm level	**display alarm history alarmlevel** *level* [**detail** | **list** | **start-number** *number*]
Query alarms by alarm time	**display alarm history alarmtime start** *start-date start-time* **end** *end-date end-time* [*start-number number*] [**detail** | **list** | **start-number** *number*]
Query alarms by alarm parameter	**display alarm history alarmparameter** { *frameid/slotid/portid* | *frameid/slotid* | *frameid* | **vlanif** *vlanif* } [**detail** | **list**]
Query all the latest alarms	**display alarm history all** [**detail** | **list**]

Table 1-48 lists the commands for querying history events.

Table 1-48 Commands for querying history events

To...	Run the Command...
Query events by event SN	**display event history eventsn** *sn* [**detail** | **list**]
Query events by event ID	**display event history eventid** *id* [**detail** | **list** | **start-number** *number*]

Copyright © Huawei Technologies Co., Ltd.

To...	Run the Command...
Query events by event type	**display event history eventtype** *type* [**detail** | **list** | **start-number** *number*]
Query events by event class	**display event history eventclass** *class* [**detail** | **list** | **start-number** *number*]
Query events by event level	**display event history eventlevel** *level* [**detail** | **list** | **start-number** *number*]
Query events by event time	**display event history eventtime start** *start-date start-time* **end** *end-date end-time* [*start-number number*] [**detail** | **list** | **start-number** *number*]
Query events by event parameter	**display event history eventparameter** { *frameid/slotid/portid* | *frameid/slotid* | *frameid* | **vlanif** *vlanif* } [**detail** | **list**]
Query all the latest events	**display event history all** [**detail** | **list**]

Procedure

Step 1 Perform an operation (such as inserting and removing a board) to generate an alarm or event.

Step 2 Run the **display alarm history** command to query history alarms.

Step 3 Run the **display event history** command to query history events.

----End

Result

You can query the alarm or event triggered by the operation you have performed.

Example

To query the history environment alarms by alarm type, do as follows:

```
huawei>display alarm history alarmtype
{ type<E><communication,service,process,equipment,environment> }:environment
{ <cr>|detail<K>|list<K>|start-number<U><1,1900>||<K> }:list
{ <cr>||<K> }:

  Command:
          display alarm history alarmtype environment list
  ------------------------------------------------------------------------
  AlarmSN  Date&Time               Alarm Name/Para
  ------------------------------------------------------------------------
  777      2009-08-21 10:18:29     The system resources usage recovers from
                                   the overload state to the normal state
                                   Resource Name: CPU, Current Percent: 70
  765      2009-08-21 10:17:29     The system resources usage exceeds the
                                   threshold
                                   Resource Name: CPU, Current Percent: 86
  764      2009-08-21 10:17:29     The system resources usage recovers from
                                   the overload state to the normal state
```


Copyright © Huawei Technologies Co., Ltd.

```
                                    Resource Name: CPU, Current Percent: 86
  714      2009-08-20 15:04:35      The system resources usage recovers from
                                    the overload state to the normal state
                                    Resource Name: CPU, Current Percent: 72
  705      2009-08-20 15:03:35      The system resources usage exceeds the
                                    threshold
                                    Resource Name: CPU, Current Percent: 86
  704      2009-08-20 15:03:35      The system resources usage recovers from
                                    the overload state to the normal state
---- More ( Press 'Q' to break ) ----
```

To query the history events by event date, and the start date is 2009-08-24, the star time is 16:00:00, the end date is 2009-08-24, and the end time is 18:00:00, do as follows:

```
huawei>display event history
{ all<K>|eventclass<K>|eventid<K>|eventlevel<K>|eventparameter<K>|eventsn<K>|eve
nttime<K>|eventtype<K> }:eventtime
{ start<K> }:start
{ start-date<D><yyyy-mm-dd> }:2009-08-24
{ start-time<T><hh:mm:ss> }:16:00:00
{ end<K> }:end
{ end-date<D><yyyy-mm-dd> }:2009-08-24
{ end-time<T><hh:mm:ss> }:18:00:00
{ <cr>|detail<K>|list<K>|start-number<U><1,1900>||<K> }:list
{ <cr>||<K> }:

  Command:
          display event history eventtime start 2009-08-24 16:00:00 end 2009-08-
24 18:00:00 list
  ------------------------------------------------------------------------
  EventSN  Date&Time                Event Name/Para
  ------------------------------------------------------------------------
  35346    2009-08-24 17:59:40      Backing up files fails from the host to
                                    the maintenance terminal
                                    FrameID: 0, SlotID: 9, Position: -1,
                                    Backup type: Host data, Backup Object:
                                    Active control board, Failure cause: Failed
                                    to transfer the file
  35345    2009-08-24 17:58:52      Change of Maintenance User's State
                                    User name: test01, Log mode: Telnet, IP:
                                    10.71.42.55, State: Log on
  35344    2009-08-24 17:58:47      Change of Maintenance User's State
                                    User name: test01, Log mode: Telnet, IP:
                                    10.71.42.55, State: Log off
  35343    2009-08-24 17:58:24      Backing up files starts from the host to
                                    the maintenance terminal
                                    FrameID: 0, SlotID: 9, Position: -1,
                                    Backup type: Host data, Backup Object:
---- More ( Press 'Q' to break ) ----
```

1.5.3 Checking the Log

If a fault occurs on the device, you can locate the fault by querying the log.

Procedure

Step 1 Perform an operation (such as adding a board) through the CLI.

Step 2 In the user mode, run the **display log** command to query the records in the log.

----End

Result

You can query the log record generated by the operation you have performed.

Copyright © Huawei Technologies Co., Ltd.

Example

To query the log records of all users within the period from 10:00:00 on 2009-08-24 to 18:00:00 on 2009-08-24, do as follows:

```
huawei>display log
{ all<K>|cli<K>|failure<K>|index<K>|memory<K>|name<K>|snmp<K> }:all
{ <cr>|start-date<D><yyyy-mm-dd> }:2009-08-24
{ -<K>|<cr>|start-time<T><hh:mm:ss> }:10:00:00
{ -<K>|<cr> }:-
{ end-date<D><yyyy-mm-dd> }:2009-08-24
{ <cr>|end-time<T><hh:mm:ss> }:18:00:00

  Command:
          display log all 2009-08-24 10:00:00 - 2009-08-24 18:00:00
  ------------------------------------------------------------------------------
  No.   UserName                            Domain            IP-Address
    65  test03                              --                10.71.42.55
  Time: 2009-08-24 17:14:48
  Cmd:  switch language-mode
  ------------------------------------------------------------------------------
  No.   UserName                            Domain            IP-Address
    64  private                             --                10.78.217.35
  Time: 2009-08-24 17:08:08
  Cmd:
  Index1: hwFrameIndex: 0
  Index2: hwSlotIndex: 9
  hwBackupServerIpAddr: 10.78.217.35
  hwBackupMode: 3
  hwBackupFileName: /bmsuser/7341374.poz
  hwBackupContent: 68
  hwBackupUserNam  ...
  ------------------------------------------------------------------------------
  No.   UserName                            Domain            IP-Address
    63  private                             --                10.78.217.35
---- More ( Press 'Q' to break ) ----
```

1.5.4 Checking the System Switchover

After the active/standby switchover is performed, the services of the active control board are switched to the standby control board. This ensures that the services run in the normal state.

Prerequisites

- An active control board and a standby control board must be configured on the device, and the cables must be connected correctly on the boards.
- The patch status of the active and standby control boards must be consistent with the hardware environment.

Precautions

- If the data of the active and standby control boards is not completely synchronized, the system prohibits the active/standby switchover.

  NOTE

  Run the **display data sync state** command to query the data synchronization status of the active and standby control boards.

- When the communication between the active and standby control boards fails or the standby control board is faulty, the system prohibits the active/standby switchover.

Copyright © Huawei Technologies Co., Ltd.

- When the data is being loaded, saved, or backed up, the system prohibits the active/standby switchover.

Context

Classification of the active/standby switchover:

According to the status of the data synchronization, the active/standby switchover is classified into the normal switchover and forced switchover.

- Normal switchover: Refers to the active/standby switchover that is performed when the data is synchronized sufficiently. A normal switchover does not cause links to break or boards to reset.
- Forced switchover: Refers to the active/standby switchover that is performed when the data is not synchronized sufficiently.

  The following data might be synchronized insufficiently:

  - Configuration data.

    When the configuration data is not fully synchronized, the system prohibits performing forced switchover by running the active/standby switchover command. Other forced switching methods, such as manually resetting the active control board or removing the active control board, cause loss of basic data or the system to reset.

    Therefore, when the configuration data is not fully synchronized, it is recommended that you do not perform the forced switchover. You can choose to reset the system. In this manner, the system can return to the normal state in a short period.
  - Basic data.

    When the basic data is not fully synchronized, the system prohibits performing forced switchover by running the active/standby switchover command. Other forced switching methods, such as manually resetting the active board or removing the active control board, neither reset the system nor affect the database, but they may cause service boards to reset.
  - Dynamic data.

    When certain dynamic data is not fully synchronized, the system permits performing forced switchover by running the active/standby switchover command. After the switchover, the on-going services continue to run in the normal state, and the original connections, alarms, and logs are not lost.

Procedure

Step 1 Run the **save** command to save the data.

Step 2 Run the **system switch-over** command to perform the active/standby switchover.

----End

Result

When the ACT LED on the original standby control board is on, log in to the system through this control board. It is found that the system runs in the normal state.

Example

After the data is saved, perform the active/standby switchover.

Copyright © Huawei Technologies Co., Ltd.

```
huawei#save
{ <cr>|configuration<K>|data<K> }:

  Command:
          save

huawei#
  It will take several minutes to save configuration file, please wait...

huawei#
  Configuration file had been saved successfully
  Note: The configuration file will take effect after being activated

huawei#
  The data is being saved, please wait a moment...
huawei(config)#system switch-over
  Are you sure to switch over? (y/n)[n]:y
```

1.6 Supplementary Information

This topic provides the commissioning supplementary information, including script making, transmission mode setting, and default software settings.

1.6.1 Script Making

Before the commissioning, you can collect the information such as the data plan according to **1.2.4 Planning Data** to make a commissioning script. Then, configure the basic data of the device by loading the script. This ensures that the device works in the normal state, which facilitates the commissioning of the basic functions and services of the device.

Script Overview

The basic configuration through the script includes but is not limited to the following items:

- Adding the power board
- Configuring the environment monitoring unit (including the FAN and the ESC)
- Configuring the route protocol

NOTE

For details about how to load the script, see **1.3.7 Loading a Configuration Script**.

Example Script

Table 1-49 lists the data plan of an example script. After the example script is configured, you can log in to the MA5600T/MA5603T/MA5608T through the maintenance terminal in the management center to commission the basic functions of the device.

Table 1-49 Script data plan

Item	Data
PRTE power board	Slot IDs: 0/21 and 0/22

Copyright © Huawei Technologies Co., Ltd.

Item	Data
FAN	● SN: 0 ● Sub-node ID: 1 (default) ● Name: FAN ● Fan speed adjustment mode: automatic
ESC	● SN: 1 ● Sub-node ID: 15 (default) ● Name: H801ESC
Route protocol	● Upstream port: 0/19/0 ● Management VLAN ID: 100; type: Standard VLAN ● IP address of the L3 interface of the management VLAN: 10.50.1.10/24 ● Gateway address: 10.50.1.1/24 ● IP address of the target network segment: 10.10.1.10/24

The following displays the commands that need to be included in the script according to the preceding data plan.

NOTICE

Each command in the script must end with a carriage return (CR).

```
enable
config
board add 0/21 H801PRTE
board add 0/22 H801PRTE
emu add 0 FAN 0 1 FAN
interface emu 0
fan speed mode automatic
quit
emu add 1 H801ESC 0 15 H801ESC
vlan 100 standard
port vlan 100 0/19 0
interface vlanif 100
ip address 10.50.1.10 24

quit
ip route-static 10.10.1.0 24 10.50.1.1


save
```

1.6.2 Configuring the File Transfer Mode

This topic describes how to configure the file transfer mode of the FTP,SFTP, Xmodem and TFTP. SFTP with high security is recommended.

Copyright © Huawei Technologies Co., Ltd.

1.6.2.1 Configuring the FTP Transfer Mode

This topic describes how to configure the FTP transfer mode for transferring (uploading or downloading) files through the inband or outband Ethernet port of the MA5600T/MA5603T/MA5608T. After the configuration, the FTP server and the MA5600T/MA5603T/MA5608T can communicate to transfer files in the FTP mode.

Prerequisites

- The Ethernet port of the FTP server is directly connected to the inband or outband Ethernet port of the MA5600T/MA5603T/MA5608T.
  - Connect to the inband Ethernet port (Upstream port) through the crossover cable.
  - Connect to the outband Ethernet port (Maintenance port) through the direct cable.
- You have logged in to the MA5600T/MA5603T/MA5608T remotely from the console (maintenance terminal), and have entered the global config mode.

Tools, Meters, and Materials

- Crossover cable
- Direct cable

Impact on System

None

Precautions

Make sure that the crossover cable is used to directly connect the FTP server to the MA5600T/MA5603T/MA5608T. In other cases, a straight-through cable is used.

Procedure

Step 1 On the FTP server, configure the IP address of its Ethernet port.

Configure the Ethernet port IP address of the FTP server according to the IP address planning in the specific networking, and ensure that the Ethernet port of the FTP server and the inband or outband Ethernet port of the MA5600T/MA5603T/MA5608T can ping each other.

For example, if the Ethernet port of the FTP server is directly connected to the MA5600T/MA5603T/MA5608T, the IP address of this Ethernet port and the IP address of the inband or outband Ethernet port of the MA5600T/MA5603T/MA5608T must be in the same subnet.

Step 2 On the FTP server, run the FTP application and set related parameters.

After running the FTP application, set the path for saving the file, FTP user name, and password.

Step 3 (This is step is used for setting the FTP user attributes for the manual file transfer.) On the MA5600T/MA5603T/MA5608T, run the **ftp set** command to set the FTP user name and password.

```
huawei(config)#ftp set
  User Name(<=40 chars):huawei
  User Password(<=40 chars):huawei//The input is not displayed on the CLI.
```


Copyright © Huawei Technologies Co., Ltd.

NOTE

By default, the FTP user name is **anonymous** and the password is **anonymous@huawei.com** in the MA5600T/MA5603T/MA5608T system.

Step 4 (Optional; this step is required when the function of database file auto-backup is used.) On the MA5600T/MA5603T/MA5608T, run the **file-server auto-backup data** command to configure the FTP user name, password, and port ID.

```
huawei(config)#file-server auto-backup data primary 10.10.20.1 ftp path test user
  User Name(<=40 chars):huawei
  User Password(<=40 chars):huawei//The input is not displayed on the CLI.
```

----End

Reference

- Any PC that runs the FTP software can serve as an FTP server.
- In the FTP file transfer mode, the user name and the password must be authenticated. Apart from setting the user name and password on the FTP server, you also need to set the FTP user name and password on the FTP client (such as the MA5600T/MA5603T/MA5608T), and make sure that the settings at both ends are the same.

1.6.2.2 Configuring the SFTP Transfer Mode

This topic describes how to configure the SFTP transfer mode for transferring (uploading or downloading) files through the inband or outband Ethernet port of the MA5600T/MA5603T/MA5608T. After the configuration, the SFTP server and the MA5600T/MA5603T/MA5608T can communicate to transfer files in the SFTP mode.

Prerequisites

- The Ethernet port of the SFTP server is directly connected to the inband or outband Ethernet port of the MA5600T/MA5603T/MA5608T.
  - Connect to the inband Ethernet port (Maintenance port) through the crossover cable.
  - Connect to the outband Ethernet port (Upstream port) through the direct cable.
- You have logged in to the MA5600T/MA5603T/MA5608T remotely from the console (maintenance terminal), and have entered the global config mode.

Tools, Meters, and Materials

- Crossover cable
- Direct cable

Impact on System

None

Precautions

Make sure that the crossover cable is used to directly connect the SFTP server to the MA5600T/MA5603T/MA5608T. In other cases, a straight-through cable is used.

Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 On the SFTP server, configure the IP address of its Ethernet port.

Configure the Ethernet port IP address of the SFTP server according to the IP address planning in the specific networking, and ensure that the Ethernet port of the SFTP server and the inband or outband Ethernet port of the MA5600T/MA5603T/MA5608T can ping each other.

For example, if the Ethernet port of the SFTP server is directly connected to the MA5600T/MA5603T/MA5608T, the IP address of this Ethernet port and the IP address of the inband or outband Ethernet port of the MA5600T/MA5603T/MA5608T must be in the same subnet.

Step 2 On the SFTP server, run the SFTP application and set related parameters.

After running the SFTP application, set the path for saving the file, SFTP user name, password, and port ID. The port ID is 22 by default.

Step 3 (This is step is used for setting the SFTP user attributes for the manual file transfer.) On the MA5600T/MA5603T/MA5608T, run the **ssh sftp set** command to set the SFTP user name, password, and port ID.

```
huawei(config)#ssh sftp set
  User Name(<=40 chars):huawei
  User Password(<=40 chars):huawei//The input is not displayed on the CLI.
  Listening Port(0--65535):22
```

NOTE

The MA5600T/MA5603T/MA5608T system does not have default SFTP user name, password, or port ID.

Step 4 (Optional; this step is required when the function of database file auto-backup is used.) On the MA5600T/MA5603T/MA5608T, run the **file-server auto-backup data** command to configure the SFTP user name, password, and port ID.

```
huawei(config)#file-server auto-backup data primary 10.10.20.1 sftp path test port
22 user
  User Name(<=40 chars):huawei
  User Password(<=40 chars):huawei//The input is not displayed on the CLI.
```

NOTE

The MA5600T/MA5603T/MA5608T system does not have default SFTP user name, password, or port ID.

----End

Reference

- Any PC that runs the SFTP software can serve as an SFTP server.
- In the SFTP file transfer mode, the user name and the password must be authenticated. Apart from setting the user name, password, and port ID on the SFTP server, you also need to set the SFTP user name, password, and port ID on the SFTP client (such as the MA5600T/MA5603T/MA5608T), and make sure that the settings at both ends are the same.

1.6.2.3 Configuring Xmodem File Transfer Mode

This topic describes how to configure the Xmodem file transfer mode. To upload or download files through the maintenance serial port on the MA5600T/MA5603T/MA5608T, configure the Xmodem file transfer mode according to this operation guide. Then, the console and the MA5600T/MA5603T/MA5608T can communicate with each other normally and transfer files in Xmodem mode.

Copyright © Huawei Technologies Co., Ltd.

Prerequisites

You must be logged in to the MA5600T/MA5603T/MA5608T from the console (also called maintenance terminal) through the serial port, and must enter the global config mode.

Tools, Meters, and Materials

RS-232 serial port cable (used for logging in to the MA5600T/MA5603T/MA5608T from the console through the serial port)

Impact on the System

None

Precautions

NOTE

- The speed of transferring files in Xmodem mode through the serial port is limited. Therefore, the system does not support file transfer in the Xmodem mode for large-size files such as program packet files and configuration files.
- It is recommended to transfer files through other modes as much as possible, such as TFTP, even if file transfer in the Xmodem mode is supported.

- The baud rate of the serial port on the MA5600T/MA5603T/MA5608T must be the same as the baud rate of the serial port on the console.
- The Xmodem transfer mode is applicable to only the active control board.
- Users who log in to the system remotely are prohibited from transferring files in Xmodem mode.

Procedure

Step 1 Query the baud rate of the serial port on the MA5600T/MA5603T/MA5608T.

```
huawei(config)#display baudrate
  Current active serial baudrate: 9600 bps
```

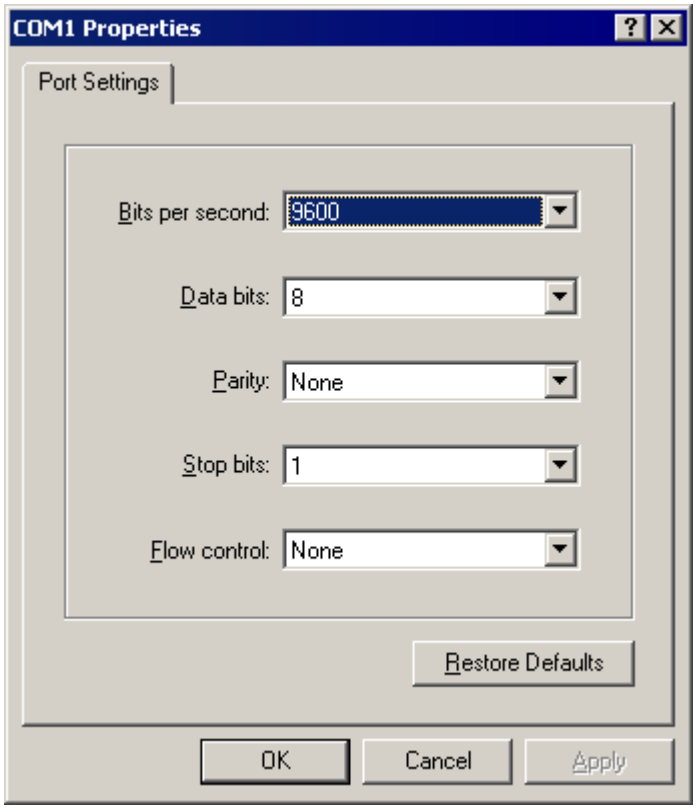
Step 2 (This step is optional but is required when you reconfigure the baud rate of the serial port.) Run the **baudrate** command on the MA5600T/MA5603T/MA5608T to configure the baud rate of the serial port on the MA5600T/MA5603T/MA5608T. The high baud rate can increase the transmission speed.

For example, reconfigure the baud rate on the MA5600T/MA5603T/MA5608T to 9600 bit/s:

```
huawei(config)#baudrate 9600
```

Step 3 Open the HyperTerminal on the console to configure the baud rate of the serial port on the console to be the same as the baud rate on the MA5600T/MA5603T/MA5608T.

Copyright © Huawei Technologies Co., Ltd.



----End

1.6.2.4 Configuring the TFTP Transfer Mode

This topic describes how to configure the TFTP transfer mode for transferring (uploading or downloading) files through the inband or outband Ethernet port of the MA5600T/MA5603T/MA5608T. After the configuration, the TFTP server and the MA5600T/MA5603T/MA5608T can communicate to transfer files in the TFTP mode.

Prerequisites

- The Ethernet port of the TFTP server is directly connected to the inband or outband Ethernet port of the MA5600T/MA5603T/MA5608T.
  - Connect to the inband Ethernet port (Maintenance port) through the crossover cable.
  - Connect to the outband Ethernet port (Upstream port) through the direct cable.
- You have logged in to the MA5600T/MA5603T/MA5608T remotely from the console (maintenance terminal), and have entered the global config mode.

Tools, Meters, and Materials

- Crossover cable
- Direct cable

Copyright © Huawei Technologies Co., Ltd.

Impact on System

None

Precautions

Make sure that the crossover cable is used to directly connect the TFTP server to the MA5600T/MA5603T/MA5608T. In other cases, a straight-through cable is used.

Procedure

Step 1 On the TFTP server, configure the IP address of its Ethernet port.

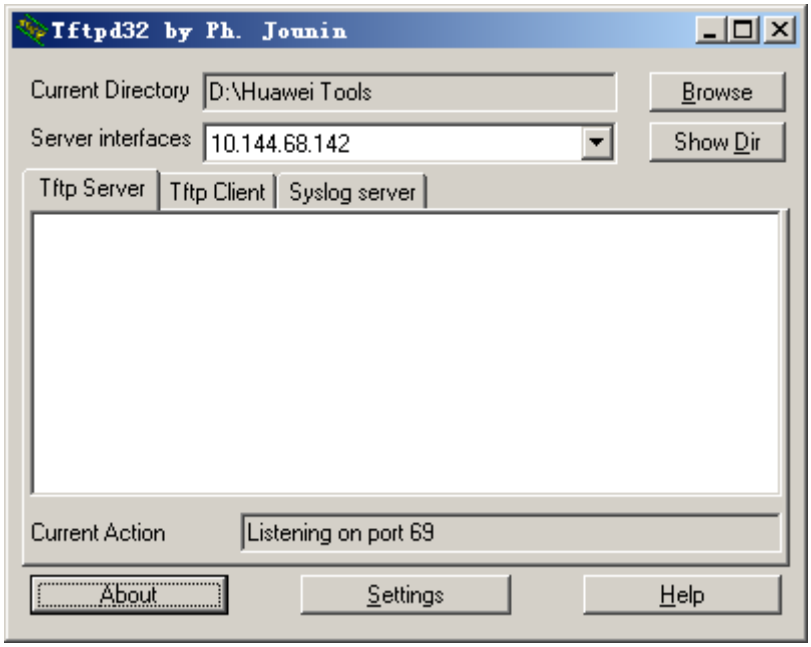
Configure the Ethernet port IP address of the TFTP server according to the IP address planning in the specific networking, and ensure that the Ethernet port of the TFTP server and the inband or outband Ethernet port of the MA5600T/MA5603T/MA5608T can ping each other.

For example, if the Ethernet port of the TFTP server is directly connected to the MA5600T/MA5603T/MA5608T, the IP address of this Ethernet port and the IP address of the inband or outband Ethernet port of the MA5600T/MA5603T/MA5608T must be in the same subnet.

Step 2 On the TFTP server, run the TFTP application and set related parameters.

1. After the TFTP application is run on the TFTP server, an interface as shown in **Figure 1-85** is displayed. In the **Server interfaces** drop-down list, select the IP address that is set in step 1.

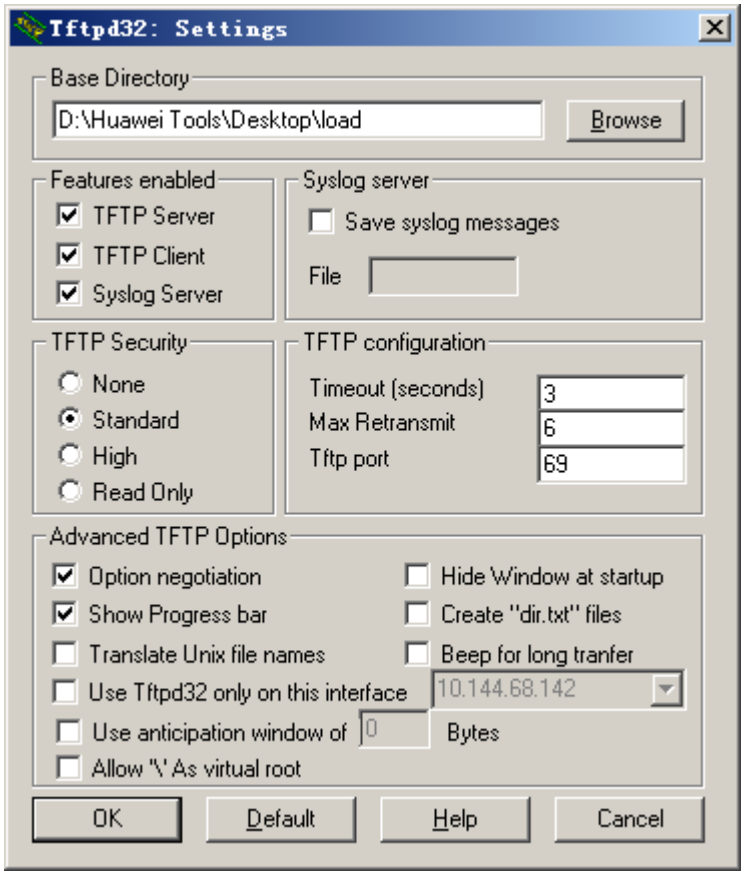
Figure 1-85 TFTP main interface



2. In the interface as shown in **Figure 1-85**, click **Settings**.
3. In the dialog box that is displayed, click **Browse** to select the path for saving the file, as shown in **Figure 1-86**.

Copyright © Huawei Technologies Co., Ltd.

Figure 1-86 Setting TFTP parameters



----End

Reference

- Any PC that runs the TFTP software can serve as a TFTP server.
- The IP address in the **Server interfaces** drop-down list is the IP address of the TFTP server. The TFTP application can identify the IP address automatically. If the TFTP server has multiple IP addresses, select the correct one.
- If the TFTP file transfer fails, check the following items:
  - Whether the selected IP address of the TFTP server is correct.
  - Whether the TFTP server can ping the inband or outband Ethernet port of the MA5600T/MA5603T/MA5608T (run the **Ping** command).
  - Whether the TFTP application is run on the TFTP server.
  - Whether the path is correctly set in the TFTP application.
  - Whether the TFTP file transfer function has been enabled through the command.
  - Whether the entered name of the file to be transferred is correct.

Copyright © Huawei Technologies Co., Ltd.

1.6.3 Software Package Settings

This topic provides the default software package settings of the MA5600T/MA5603T/MA5608T.

1.6.3.1 Factory Default of the xDSL Line Profile

The following **Table 1-50**, **Table 1-51**, **Table 1-52** list the factory defaults of the xDSL line profile on the MA5600T/MA5603T/MA5608T.

Table 1-50 ADSL line profile

Profile Index	Profile	Parameter	Factory Default
1	DEFVAL	Transmission mode	T1.413 ETSI G.992.1(Annex A/B/C) G.992.2(Annex A/C) G.992.3(Annex A/B/I/J/L/M) G.992.4(Annex A/I) G.992.5(Annex A/B/I/J/M)
		Trellis mode	Enable
		Bit swap downstream	Enable
		Bit swap upstream	Enable
		Form of transmit rate adaptation downstream	AdaptAtStartup
		Form of transmit rate adaptation upstream	AdaptAtStartup
		Target SNR margin downstream (0.1dB)	60
		Minimum SNR margin downstream (0.1dB)	0
		Maximum SNR margin downstream(0.1dB)	160
		Target SNR margin upstream (0.1dB)	60
		Minimum SNR margin upstream (0.1dB)	0
		Maximum SNR margin upstream (0.1dB)	160

Copyright © Huawei Technologies Co., Ltd.

Profile Index	Profile	Parameter		Factory Default
		Allow transition to idle		not allowed
		Allow transition to low power		not allowed
		L0 time(second)		255
		Layer 2 time(second)		30
		Layer 3 time(second)		255
		Maximum aggregate transmit power reduction(dB)		3
		Total maximum aggregate transmit power reduction(dB)		9
		INM inter arrival time offset downstream(symbol):		3
		INM inter arrival time step downstream		0
		INM cluster continuation value downstream(symbol)		0
		INM equivalent INP mode downstream		0
		<defmode>	Maximum nominal transmit PSD downstream(-0.1dBm)	400
			Maximum nominal transmit PSD upstream (-0.1dBm)	380
			Maximum nominal aggregate transmit power downstream(0.1dBm)	200
			Maximum nominal aggregate transmit power upstream(0.1dBm)	125
			Upstream PSD mask selection	ADLU-32/EU-32
		Network timing reference clock mode		FreeRun

Copyright © Huawei Technologies Co., Ltd.

Table 1-51 VDSL line profile

Profile Index	Profile	Parameter	Factory Default
1	DEFVAL	Transmission mode	T1.413 G.992.1(Annex A/B/C) G.992.2(Annex A/C) G.992.3(Annex A/B/I/J/L/M) G.992.4(Annex A/I) G.992.5(Annex A/B/I/J/M) G.993.2(Annex A/B/C)
		Bit swap downstream	Enable
		Bit swap upstream	Enable
		Form of transmit rate adaptation downstream	AdaptAtStartup
		Form of transmit rate adaptation upstream	AdaptAtStartup
		Target SNR margin downstream(0.1dB)	60
		Minimum SNR margin downstream(0.1dB)	0
		Maximum SNR margin downstream (0.1dB)	300
		Target SNR margin upstream(0.1dB)	60
		Minimum SNR margin upstream(0.1dB)	0
		Maximum SNR margin upstream(0.1dB)	300
		UPBO US1 band reference PSD parameters [a, b]	1650,1020
		UPBO US2 band reference PSD parameters [a, b]	1650,615
		UPBO US3 band reference PSD parameters [a, b]	0,0
		UPBO US4 band reference PSD parameters [a, b]	0,0
		UPBO Boost Mode	Enable
		UPBO US1 band reference electrical length	0

Copyright © Huawei Technologies Co., Ltd.

Profile Index	Profile	Parameter		Factory Default
		UPBO US2 band reference electrical length		0
		UPBO US3 band reference electrical length		0
		UPBO US4 band reference electrical length		0
		UPBO use of electrical length to compute UPBO		Auto
		Allow transition to idle		not allowed
		Allow transition to low power		not allowed
		L0 time(second)		255
		Layer 2 time(second)		30
		Layer 3 time(second)		255
		Maximum aggregate transmit power reduction(dB)		3
		Total maximum aggregate transmit power reduction(dB)		9
		<defmode>	G.993.2 profile	Profile12a
			VDSL2 PSD class mask	AnnexB998-M2x-B (B8-6)
			VDSL2 link use of U0	Unused
			Maximum nominal aggregate transmit power downstream (0.1dBm)	145
			Maximum nominal aggregate transmit power upstream (0.1dBm)	145
			Upstream PSD mask selection	ADLU-32/EU-32
			Virtual noise mode downstream	Disable
			Virtual noise mode upstream	Disable
		Network timing reference clock mode		FreeRun
		INM inter arrival time offset downstream (symbol)		3
		INM inter arrival time step downstream		0
		INM cluster continuation value downstream (symbol)		0

Copyright © Huawei Technologies Co., Ltd.

Profile Index	Profile	Parameter	Factory Default
		INM equivalent INP mode downstream	0
		INM inter arrival time offset upstream (symbol)	3
		INM inter arrival time step upstream	0
		INM cluster continuation value upstream (symbol)	0
		INM equivalent INP mode upstream	0
		SOS time Window downstream(64ms)	0
		Minimum percentage of degraded tones downstream	0
		Minimum number of normalized CRC anomalies downstream(0.02)	65535
		Maximum number of SOS downstream	0
		SNR margin offset of ROC downstream (0.1dB)	0
		Minimum impulse noise protection of ROC downstream	0
		SOS time Window upstream(64ms)	0
		Minimum percentage of degraded tones upstream	0
		Minimum number of normalized CRC anomalies upstream(0.02)	65535
		Maximum number of SOS upstream	0
		SNR margin offset of ROC upstream (0.1dB)	0
		Minimum impulse noise protection of ROC upstream	0

Table 1-52 SHDSL line profile

Profile Index	Profile	Parameter	Factory Default
1	DEFVAL	Path mode	ATM
		G.SHDSL interface mode of line	two wire

Copyright © Huawei Technologies Co., Ltd.

Profile Index	Profile	Parameter	Factory Default
		G.SHDSL minimum line rate (unit:kbps)	2048
		G.SHDSL maximum line rate (unit:kbps)	2048
		PSD	symmetric
		Transmission mode	all
		Remote enable	enabled
		Probe enable	disabled
		Downstream current target SNR margin	6
		Downstream worst target SNR margin	0
		Upstream current target SNR margin	6
		Upstream worst target SNR margin	0
		Target SNR margin used bitmap	0x5
		Reference times	0

1.6.3.2 Factory Defaults of the xDSL Alarm Profile

The following **Table 1-53**, **Table 1-54**, **Table 1-55** list the factory defaults of the xDSL alarm profile on the MA5600T/MA5603T/MA5608T.

Table 1-53 ADSL alarm profile

Profile Index	Profile	Parameter		Factory Default
1	DEFVAL	CO	The number of forward error correction seconds	0
			The number of errored seconds	0
			The number of severely errored seconds	0
			The number of loss of signal seconds	0
			The number of unavailable seconds	0
		CPE	The number of forward error correction seconds	0
			The number of errored seconds	0

Copyright © Huawei Technologies Co., Ltd.

Profile Index	Profile	Parameter		Factory Default
			The number of severely errored seconds	0
			The number of loss of signal seconds	0
			The number of unavailable seconds	0
			The number of failed full initialization	0
			The number of failed short initialization	0

Table 1-54 VDSL alarm profile

Profile Index	Profile	Parameter		Factory Default
1	DEFVAL	CO	The number of forward error correction seconds	0
			The number of errored seconds	0
			The number of severely errored seconds	0
			The number of loss of signal seconds	0
			The number of unavailable seconds	0
		CPE	The number of forward error correction seconds	0
			The number of errored seconds	0
			The number of severely errored seconds	0
			The number of loss of signal seconds	0
			The number of unavailable seconds	0
		The number of failed full initialization		0
		The number of full initialization		0

Copyright © Huawei Technologies Co., Ltd.

Table 1-55 SHDSL alarm profile

Profile Index	Profile	Parameter	Factory Default
1	DEFVAL	Loop attenuation threshold (unit:dB)	0
		SNR margin threshold (unit:dB)	0
		ES threshold (unit:second)	0
		SES threshold (unit:second)	0
		CRC anomaly threshold	0
		LOSWS threshold (unit:second)	0
		UAS threshold (unit:second)	0
		Dying gasp alarm switch	Enable
		Reference status	Unused

1.6.3.3 Default settings of the system parameters

The following table lists the default settings of the system parameters on the MA5600T/MA5603T/MA5608T.

Table 1-56 System parameters

Index	Description	Default
0	Sending howler tone flag, 0:not send, 1:send	1
1	Overseas version flag, 0:China, 1:HongKong, 2:Brazil, 3:Egypt, 4:Singapore, 5:Thailand, 6:France, 7:Britain MSFUK, 8:Britain ETSI, 9:Bulgaria	0
2	Stop initial ringing flag, 0:not send, 1:send	0
3	The mode of voicemail, 0:high voltage, 1:FSK and ring, 2:FSK no ring	1
4	Global digitmap support flag 0:Not support, 1:Support	1
5	Transfer mode of media stream in a device, 0:Device internal forwarding, 1:Device external forwarding	0
6	RTP 2833 Payload Type	97

Copyright © Huawei Technologies Co., Ltd.

1.6.3.4 Default settings of the overseas parameters

The following table lists the default settings of the overseas parameters on the MA5600T/MA5603T/MA5608T.

Table 1-57 Overseas parameters

Index	Description	Default
0	Hooking upper threshold(ms), reference: China:350, HongKong:800	350
1	Hooking lower threshold(ms), reference: China:100, HongKong:100	100
2	Flag of applying PARKED LINE FEED or not when user port is locked, 0:not apply, 1:apply	0

1.6.3.5 Factory Defaults of a DBA Profile

The following table lists the factory defaults of a DBA profile on the MA5600T/MA5603T/MA5608T.

Table 1-58 DBA profile 1

Profile Name	Default
Profile-name	dba-profile_1
Profile-ID	1
Type	1
Bandwidth compensation	No
Fix bandwidth(kbps)	5120
Assure bandwidth(kbps)	0
Maximum bandwidth(kbps)	0

Table 1-59 DBA profile 2

Profile Name	Default
Profile-name	dba-profile_2
Profile-ID	2
Type	1
Bandwidth compensation	No

Copyright © Huawei Technologies Co., Ltd.

Profile Name	Default
Fix bandwidth(kbps)	1024
Assure bandwidth(kbps)	0
Maximum bandwidth(kbps)	0

Table 1-60 DBA profile 3

Profile Name	Default
Profile-name	dba-profile_3
Profile-ID	3
Type	4
Bandwidth compensation	No
Fix bandwidth(kbps)	0
Assure bandwidth(kbps)	0
Maximum bandwidth(kbps)	32768

Table 1-61 DBA profile 4

Profile Name	Default
Profile-name	dba-profile_4
Profile-ID	4
Type	1
Bandwidth compensation	No
Fix bandwidth(kbps)	1024000
Assure bandwidth(kbps)	0
Maximum bandwidth(kbps)	0

Table 1-62 DBA profile 5

Profile Name	Default
Profile-name	dba-profile_5
Profile-ID	5

Copyright © Huawei Technologies Co., Ltd.

Profile Name	Default
Type	1
Bandwidth compensation	No
Fix bandwidth(kbps)	32768
Assure bandwidth(kbps)	0
Maximum bandwidth(kbps)	0

Table 1-63 DBA profile 6

Profile Name	Default
Profile-name	dba-profile_6
Profile-ID	6
Type	1
Bandwidth compensation	No
Fix bandwidth(kbps)	102400
Assure bandwidth(kbps)	0
Maximum bandwidth(kbps)	0

Table 1-64 DBA profile 7

Profile Name	Default
Profile-name	dba-profile_7
Profile-ID	7
Type	2
Bandwidth compensation	No
Fix bandwidth(kbps)	0
Assure bandwidth(kbps)	32768
Maximum bandwidth(kbps)	0

Copyright © Huawei Technologies Co., Ltd.

Table 1-65 DBA profile 8

Profile Index	Profile Name	Default
8	Profile-name	dba-profile_8
	Profile-ID	8
	Type	2
	Bandwidth compensation	No
	Fix bandwidth(kbps)	0
	Assure bandwidth(kbps)	102400
	Maximum bandwidth(kbps)	0

Table 1-66 DBA profile 9

Profile Name	Default
Profile-name	dba-profile_9
Profile-ID	9
Type	3
Bandwidth compensation	No
Fix bandwidth(kbps)	0
Assure bandwidth(kbps)	32768
Maximum bandwidth(kbps)	65536

1.6.3.6 Default settings of the GPON ONT line profile

The following table lists the default settings of the GPON ONT line profile on the MA5600T/MA5603T/MA5608T.

Table 1-67 GPON ONT line profile

Parameter Name	Default
FEC upstream switch	Disable
Qos mode	PQ
Mapping mode	VLAN
<T-CONT 0>	DBA Profile-ID:1

Copyright © Huawei Technologies Co., Ltd.

1.6.3.7 Default settings of the GPON ONT service profile

The following table lists the default settings of the GPON ONT service profile on the MA5600T/MA5603T/MA5608T.

Table 1-68 GPON ONT service profile

Parameter Name		Default	
Port-type	POTS	Port-number	0
	ETH		0
	TDM		0
	MOCA		0
	CATV		0
TDM port type		E1	
TDM service type		TDMoGem	
MAC learning function switch		Enable	
ONT transparent function switch		Disable	
Multicast forward mode		Unconcern	
Multicast forward VLAN		-	
Multicast mode		Unconcern	
Upstream IGMP packet forward mode		Unconcern	
Upstream IGMP packet forward VLAN		-	

1.6.3.8 Factory Defaults of a GPON ONT Alarm Profile

The following table lists the factory defaults of a GPON ONT alarm profile on the MA5600T/MA5603T/MA5608T.

Table 1-69 GPON ONT alarm profile

Profile Index	Profile	Parameter	Factory Default
1	alarm-profile_1	GEM port loss of packets threshold	0
		GEM port misinserted packets threshold	0

Copyright © Huawei Technologies Co., Ltd.

Profile Index	Profile	Parameter	Factory Default
		GEM port impaired blocks threshold	0
		Ethernet FCS errors threshold	0
		Ethernet excessive collision count threshold	0
		Ethernet late collision count threshold	0
		Too long Ethernet frames threshold	0
		Ethernet buffer (Rx) overflows threshold	0
		Ethernet buffer (Tx) overflows threshold	0
		Ethernet single collision frame count threshold	0
		Ethernet multiple collisions frame count threshold	0
		Ethernet SQE count threshold	0
		Ethernet deferred transmission count threshold	0
		Ethernet internal MAC Tx errors threshold	0
		Ethernet carrier sense errors threshold	0
		Ethernet alignment errors threshold	0
		Ethernet internal MAC Rx errors threshold	0
		PPPOE filtered frames threshold	0
		MAC bridge port discarded frames due to delay threshold	0
		MAC bridge port MTU exceeded discard frames threshold	0
		MAC bridge port received incorrect frames threshold	0
		CES general error time threshold	0
		CES severely time threshold	0
		CES bursty time threshold	0

Copyright © Huawei Technologies Co., Ltd.

Profile Index	Profile	Parameter	Factory Default
		CES controlled slip time threshold	0
		CES unavailable time threshold	0
		Drop events threshold	0
		Undersize packets threshold	0
		Fragments threshold	0
		Jabbers threshold	0
		Failed signal of ONU threshold (Format:1e-x)	3
		Degraded signal of ONU threshold (Format:1e-x)	4

1.6.3.9 Default settings of the environment monitoring units

Tables **Table 1-70**, **Table 1-71** list the default settings of the environment monitoring units on the MA5600T/MA5603T/MA5608T.

Table 1-70 Default settings of the H801ESC board

Parameter	Default
Sub-node	15
Analog parameters	ESC analog parameter IDs ● 0: allocated to the temperature sensor by default (unable to be changed by the user). ● 1-4: allocated to the voltage sensor by default. – 1 indicates -48 V input of channel 0. – 2 indicates -48 V input of channel 1. – 3 indicates -48 V input of channel 2. – 4 indicates -48 V input of channel 3. ● 5-8: user-defined analog parameters allocated to other extended analog sensors, such as the humidity sensor.
	Upper and lower alarm thresholds ● Temperature: 5°C to 55°C ● Humidity: 0% RH to 80% RH

Copyright © Huawei Technologies Co., Ltd.

Parameter	Default
Digital parameters	ESC digital parameter IDs ● Allocated by default (unable to be changed by the user) – 0: MDF – 1: door status sensor 0 – 9: water – 10-13: lightning arresters 0-3 – 14-15: switches 11 and 12 – 16-17: switches 21 and 22 – 18-19: switches 31 and 32 – 20-21: switches 41 and 42 – 22: external sensor power ● User-defined IDs – 2-8: allocated to other extended digital sensors.
	Definition of user-defined alarm indexes 1: AC voltage; 2: AC switch; 3: battery voltage; 4: battery fuse; 5: load fuse; 6: rectifier unit; 7: secondary power supply; 8: door status of the cabinet; 9: door status of the equipment room; 10: window; 11: theft; 12: MDF; 13: fan; 14: fire; 15: smoke; 16: water; 17: diesel; 18: abnormal smell 19: air conditioner; 20: lightning arrester; 21: user-defined alarms of digital parameters

Table 1-71 Default settings of the FAN

Parameter	Default
Sub-node	1
Fan speed adjustment mode	Automatic
Whether to report the fan alarm	Permit

Table 1-72 Default settings of the TCU

Parameter	Default
Sub-node	7

Copyright © Huawei Technologies Co., Ltd.

2 Basic Configurations

About This Chapter

Basic configurations mainly include certain common configurations, public configurations, and pre-configurations in service configurations. There is no obvious logical relation between basic configurations. You can perform basic configurations according to actual requirements.

2.1 Configuring Alarms
Alarm management includes the following functions: alarm record, alarm setting, and alarm statistics. These functions help you to maintain the device and ensure that the device works efficiently.

2.2 Adding Port Description
This topic describes how to add port description.

2.3 Configuring the Attributes of an Upstream Ethernet Port
This topic describes how to configure the attributes of a specified Ethernet port so that the system communicates with the upstream device in the normal state.

2.4 Configuring AAA
This topic describes how to configure the AAA on the MA5600T/MA5603T/MA5608T, including configuring the MA5600T/MA5603T/MA5608T as the local and remote AAA servers.

2.5 Configuring DOCSIS Event Reporting
DOCSIS 3.0 defines various DOCSIS events, such as authentication failure and CM certificate error events. Configuring DOCSIS event reporting helps you obtain MA5600T/MA5603T/MA5608T and CM running status.

Copyright © Huawei Technologies Co., Ltd.

2.1 Configuring Alarms

Alarm management includes the following functions: alarm record, alarm setting, and alarm statistics. These functions help you to maintain the device and ensure that the device works efficiently.

Context

An alarm refers to the notification of the system after a fault is detected. After an alarm is generated, the system broadcasts the alarm to the terminals, mainly including the NMS and command line interface (CLI) terminals.

Alarms are classified into fault alarm and recovery alarm. After a fault alarm is generated at a certain time, the fault alarm lasts till the fault is rectified to clear the alarm.

You can modify the alarm settings according to your requirements. The settings are alarm severity, alarm output mode through the CLI and alarm statistics switch.

When managing alarms on the GUI through the NMS, you can set filtering criteria to mask unimportant alarms and events. Such filtering function facilitates the focus of the important alarms and eliminates the load of the NMS.

Procedure

- Clear alarms.

  You can run the **alarm active clear** command to clear the alarms that are not recovered in the system.

  - When an active alarm lasts a long time, you can run this command to clear the alarm.
  - Before clearing an alarm, you can run the **display alarm active** command to query the currently active alarms.

- Configure alarm level.

  Run the **alarm alarmlevel** command to configure the alarm level.

  - Alarm levels are critical, major, minor, and warning.
  - Parameter **default** indicates restoring the alarm level to the default setting.
  - You can run the **display alarm list** command to query the alarm level.
  - The system specifies the default (also recommended) alarm level for each alarm. Use the default alarm level unless otherwise required.

- Configure alarm jitter-proof.

  Run the **alarm jitter-proof** command to configure the alarm jitter-proof function and the jitter-proof period.

  - To prevent a fault alarm and its recovery alarm from being displayed frequently, you can enable the alarm jitter-proof function to filter alarms in the system.
  - After the alarm jitter-proof function is enabled, the alarm in the system is not reported to the NMS immediately but is reported to the NMS after an alarm jitter-proof period.
  - If an alarm is recovered in an alarm jitter-proof period, the alarm is not reported to the NMS.

Copyright © Huawei Technologies Co., Ltd.

- You can run the **display alarm jitter-proof** command to check whether the alarm jitter-proof function is enabled and whether the alarm jitter-proof period is set.
- By default, the alarm jitter-proof function is disabled. You can determine whether to enable the function according to the running of the device.

- Set or shield the output of alarms.

  Run the **(undo) alarm output** command to set or shield the output of alarms to the CLI terminal.

  - Setting the output mode of alarms does not affect the generating of alarms. The alarms generated by the system are still recorded. You can run the **display alarm history** command to query the alarms that are shielded.
  - When the new output mode of an alarm conflicts with the previous mode, the new output mode takes effect.
  - The output mode of the recovery alarm is the same as the output mode of the fault alarm. When the output mode of the fault alarm is set, the system automatically synchronizes the output mode of its recovery alarm. The reverse is also applicable.

- Set alarm statistics period.

  Run the **alarm-event statistics period** command to set the alarm statistics collection period.

  - You can use the statistical result of alarms and events to locate a problem in the system.
  - You can run the **display alarm statistics** command to query the alarm statistical record.

- Filter alarms reporting to NMS.

  Run the **trap filter alarm condition** command to filter alarms that the device reports to the NMS through traps.

  The filtering criteria can be alarm ID, alarm severity, alarm type, subrack ID, subrack ID/slot ID, subrack ID/slot ID/port ID, VLAN interface, and NE.

  To reduce alarms and avoid alarm storms, the system does not send alarms of some ONTs to the NMS. To query the filtering criteria of alarms and events in the system, run the **display trap filter** command.

- Query alarm configuration and alarm statistics.

  Run the **display alarm configuration** command to query the alarm configuration according to the alarm ID. The alarm configuration that you can query includes the alarm ID, alarm name, alarm class, alarm type, alarm level, default alarm level, number of parameters, CLI output flag, conversion flag, and detailed alarm description.

  Run the **display alarm statistics** command to query the alarm statistical record.

  - When you need to know the frequency in which one alarm occurs within a time range, and to know the working conditions of the device and analyze the fault that may exist, run this command.
  - Currently, you can query the alarm statistics in the current period and previous period in the system.

- (Optional) Configure alarm policy for ONT.

  In FTTH scenarios, you can configure the ONT alarm policy profile to configure alarms for different service policies.

  1. Create an ONT alarm policy profile.

Copyright © Huawei Technologies Co., Ltd.

Run the **ont-alarm-policy** command to create an ONT alarm policy profile.

The system supports a maximum number of 16 alarm policy profiles. The default alarm policy profile is profile 0.

It is recommended that you configure different alarm policies for VIP and common users.

2. Configure attributes of the ONT alarm policy profile.

   Run the **alarm filter** command to configure the control function of each alarm of the profile.

   Run the **commit** command to save the configuration.

   Run the **display ont-alarm-policy** command to query attributes of the ONT alarm policy profile.

3. Bind the ONT to the ONT alarm policy profile.

   Run the **ont alarm-policy** command to bind the ONT to the ONT alarm policy profile so that the PON board can control whether to send the ONT alarm information.

   During ONT adding or confirmation, the system binds the ONT to the default ONT alarm policy profile 0.

----End

Example

Assume the following configurations: The output of all alarms at level **warning** is shielded to the CLI terminal, the alarm jitter-proof function is enabled, the alarm jitter-proof period is set to 15s, the level of alarms with IDs 0x0a310021 and 0x2e314021 are modified to **critical**, do as follows:

```
huawei(config)#undo alarm output alarmlevel warning
huawei(config)#alarm jitter-proof on
huawei(config)#alarm jitter-proof 15
huawei(config)#alarm alarmlevel 0x0a310021 critical
huawei(config)#alarm alarmlevel 0x2e314021 critical
```

To mask the activation and deactivation alarm events of the ADSL port (event IDs 0x0a300013 and 0x0a300015) so that normal operations are not affected by too many alarms, do as follows:

```
huawei(config)#undo event output eventid 0x0a300013
huawei(config)#undo event output eventid 0x0a300015
```

To create ONT alarm policy profile 10, filter the following alarms, and bind this profile to GPON ONT 1 connected to port 0/3/0, do as follows:

- 0x2e112003 (The signal degrade of ONTi (SDi) occurs)
- 0x2e112004 (The signal fail of ONTi (SFi) occurs)
- 0x2e112006 (The loss of frame of ONTi (LOFi) occurs)
- 0x2e313015 (The hardware of the ONT is faulty)
- 0x2e313016 (The ONT switches to the standby battery)
- 0x2e313017 (The standby battery of the ONT is lost)
- 0x2e313018 (The standby battery of the ONT cannot be charged)

Copyright © Huawei Technologies Co., Ltd.

- 0x2e313019 (The voltage of the standby battery of the ONT is too low)
- 0x2e31301a (The shell of the ONT is opened)
- 0x2e313024 (The loss of signals occurs on the ethernet port of the ONT)
- 0x2e313025 (No signal is received in the video UNI of the ONT)
- 0x2e31302a (The E1/T1 port loss of signal (LOS) occurs at the ONT)

```
huawei(config)#ont-alarm-policy policy-id 10
huawei(config-ont-alarm-policy-10)#alarm filter 0x2e112003
huawei(config-ont-alarm-policy-10)#alarm filter 0x2e112004
huawei(config-ont-alarm-policy-10)#alarm filter 0x2e112006
huawei(config-ont-alarm-policy-10)#alarm filter 0x2e313015
huawei(config-ont-alarm-policy-10)#alarm filter 0x2e313016
huawei(config-ont-alarm-policy-10)#alarm filter 0x2e313017
huawei(config-ont-alarm-policy-10)#alarm filter 0x2e313018
huawei(config-ont-alarm-policy-10)#alarm filter 0x2e313019
huawei(config-ont-alarm-policy-10)#alarm filter 0x2e31301a
huawei(config-ont-alarm-policy-10)#alarm filter 0x2e313024
huawei(config-ont-alarm-policy-10)#alarm filter 0x2e313025
huawei(config-ont-alarm-policy-10)#alarm filter 0x2e31302a
huawei(config-ont-alarm-policy-10)#commit
huawei(config-ont-alarm-policy-10)#quit
huawei(config)#interface gpon 0/3
huawei(config-if-gpon-0/3)#ont alarm-policy 0 1 policy-id 10
```

2.2 Adding Port Description

This topic describes how to add port description.

Prerequisites

A board must be added to the system.

Context

After the description of a physical port on the board is added, the description facilitates information query in system maintenance.

Procedure

Step 1 In the global config mode, run the **port desc** command to add port description.

Port description is a character string, used to identify a port on a board in a slot of a subrack.

Step 2 Run the **display port desc** command to query port description.

----End

Example

Plan the format of user port description as "community ID-building ID-floor ID/subrack ID-slot ID-port ID". "Community ID-building ID-floor ID" indicates the physical location where the user terminal is deployed, and subrack ID-slot ID-port ID" indicates the physical port on the local device that is connected to the user terminal. This plan can present the user terminal location and the connection between the user terminal and the device, which facilitates query in maintenance. Assume that the user terminal that is connected to port 0/2/0 of the MA5600T/

Copyright © Huawei Technologies Co., Ltd.

MA5603T/MA5608T is deployed in floor 1, building 01 of community A. To add port description according to the plan, do as follows:

```
huawei(config)#port desc 0/2/0 description A-01-01/0-2-0
huawei(config)#display port desc 0/2/0
  ------------------------------------------------------------
   F/ S/ P   IMA Group   Port Description
  ------------------------------------------------------------
   0/ 2/ 0   -           A-01-01/0-2-0
  ------------------------------------------------------------
```

2.3 Configuring the Attributes of an Upstream Ethernet Port

This topic describes how to configure the attributes of a specified Ethernet port so that the system communicates with the upstream device in the normal state.

Prerequisites

The board in the GIU slot must be in position and must work in the normal state.

Context

The MA5600T/MA5603T/MA5608T should be interconnected with the upstream device through the Ethernet port. Therefore, pay attention to the consistency of port attributes.

Default Configuration

Table 2-1 lists the default settings of the attributes of an Ethernet port.

Table 2-1 Default settings of the attributes of an Ethernet port

Parameter	Auto-negotiation mode of the port	Port rate	Duplex mode	Network cable adaptation mode	Flow control
Default Setting (Optical Port)	● GICD/ GICF/ GICK: enabled ● Other GIU board: disabled	● FE optical port: 100 Mbit/s ● GE optical port: 1000 Mbit/s ● 10GE optical port: 10000 Mbit/s	Full-duplex, read only	Not supported	Disabled

Copyright © Huawei Technologies Co., Ltd.

Parameter	Auto-negotiation mode of the port	Port rate	Duplex mode	Network cable adaptation mode	Flow control
Default Setting (Electrical Port)	Enabled	NA **NOTE** After the auto-negotiation mode of the port is disabled, you can configure the port rate.	NA **NOTE** After the auto-negotiation mode of the port is disabled, you can configure the duplex mode.	● FE electrical port: auto ● GE electrical port: normal	Disabled

Procedure

- Configure the physical attributes of an Ethernet port.
  1. (Optional) Set the auto-negotiation mode of the Ethernet port.

     Run the **auto-neg** command to set the auto-negotiation mode of the Ethernet port. You can enable or disable the auto-negotiation mode:

     - After the auto-negotiation mode is enabled, the port automatically negotiates with the peer port for the rate and working mode of the Ethernet port.
     - After the auto-negotiation mode is disabled, the rate and working mode of the port are in the forced mode (adopt default values or are set through command lines).

     NOTICE

     The mode (auto-negotiation mode or forced mode) of the OLT port must be consistent with that of the interworking port. Otherwise, the communication fails.

  2. (Optional) Set the rate of the Ethernet port.

     Run the **speed** command to set the rate of the Ethernet port. After the port rate is set successfully, the port works at the set rate. Pay attention to the following points:

     - Make sure that the rate of the Ethernet port is the same as that of the interconnected port on the peer device. This prevents communication failure.
     - The auto-negotiation mode should be disabled.

  3. (Optional) Set the duplex mode of the Ethernet port.

     Run the **duplex** command to set the duplex mode of the Ethernet port. The duplex mode of an Ethernet port can be full-duplex, half-duplex, or auto negotiation. Pay attention to the following points:

     - Make sure that the ports of two interconnected devices work in the same duplex modes. This prevents communication failure.

Copyright © Huawei Technologies Co., Ltd.

- The auto-negotiation mode should be disabled.
- The duplex mode of optical ports does not support configuration.

4. (Optional) Configure the network cable adaptation mode of the Ethernet port.

   Run the **mdi** command to configure the network cable adaptation mode of the Ethernet port to match the actual network cable. The network adaptation modes are as follows:

   - **normal**: Specifies the adaptation mode of the network cable as straight-through cable. In this case, the network cable connecting to the Ethernet port must be a straight-through cable.
   - **across**: Specifies the adaptation mode of the network cable as crossover cable. In this case, the network cable connecting to the Ethernet port must be a crossover cable.
   - **auto**: Specifies the adaptation mode of the network cable as auto-sensing. The network cable can be a straight-through cable or crossover cable.

   Pay attention to the following points:

   - The Ethernet optical port does not support the network cable adaptation mode.
   - If the Ethernet electrical port works in forced mode (auto-negotiation mode disabled), the network cable type of the port cannot be configured to **auto**.

- Configure flow control on the Ethernet port.

  Run the **flow-control** command to enable flow control on the Ethernet port. When the flow of an Ethernet port is heavy, run this command to control the flow to prevent network congestion, which may cause the loss of data packets. Flow control should be supported on both the local and peer devices. Pay attention to the following points:

  - If the peer device does not support flow control, generally, enable flow control on the local device.
  - If the peer device supports flow control, generally, disable flow control on the local device.

  By default, flow control is disabled.

- Mirror the Ethernet port.

  Run the **mirror port** command to mirror the Ethernet port. When the system is faulty, copy the traffic of a certain port to the other port and output the traffic for traffic observation, network fault diagnosis, and data analysis.

----End

Example

Ethernet port 0/19/0 is an electrical port. The attribute is as follows: The port rate is 1000 Mbit/s in duplex mode, with supporting flow control, not supporting auto-negotiation function. Do as follows:

```
huawei(config)#interface 0/19
huawei(config-if-0/19)#auto-neg 0 disable
huawei(config-if-0/19)#speed 0 1000
huawei(config-if-0/19)#duplex 0 full
huawei(config-if-0/19)#flow-control 0
```


Copyright © Huawei Technologies Co., Ltd.

2.4 Configuring AAA

This topic describes how to configure the AAA on the MA5600T/MA5603T/MA5608T, including configuring the MA5600T/MA5603T/MA5608T as the local and remote AAA servers.

Context

AAA refers to authentication, authorization, and accounting. In the process that a user accesses network resources, through AAA, certain rights are authorized to the user if the user passes authentication, and the original data about the user accessing network resources is recorded.

- Authentication: Checks whether a user is allowed to access network resources.
- Authorization: Determines what network resources a user can access.
- Accounting: Records the original data about the user accessing network resources.

Application Context

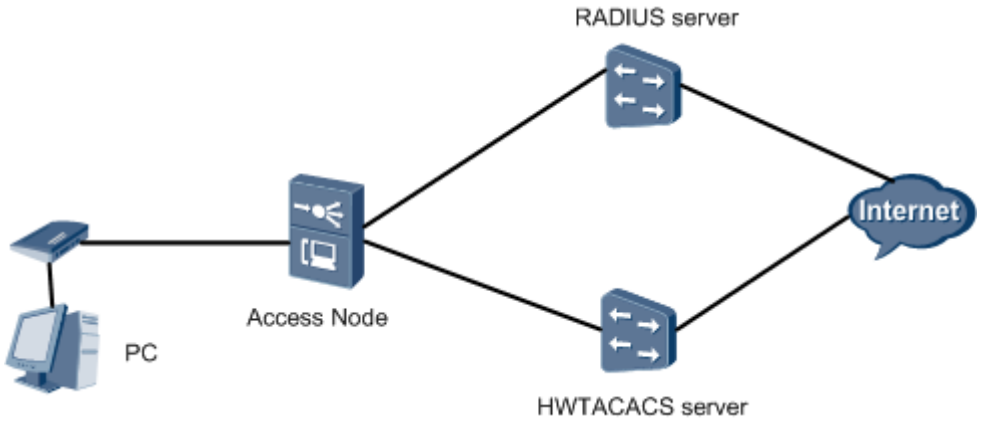
AAA is generally applied to the users that access the Internet in the PPPoA, PPPoE, 802.1x, VLAN, WLAN, ISDN, or Admin SSH (associating the user name and the password with the domain name) mode.

NOTE

In the existing network, 802.1x and Admin SSH correspond to the local AAA, that is, the MA5600T/MA5603T/MA5608T functions as a local AAA server; PPPoE corresponds to the remote AAA, that is, the MA5600T/MA5603T/MA5608T functions as the client of a remote AAA server.

Figure 2-1 shows an example network of the AAA application.

Figure 2-1 Example network of the AAA application



The preceding figure shows that the AAA function can be implemented on the MA5600T/MA5603T/MA5608T in the following three ways:

- The MA5600T/MA5603T/MA5608T functions as a local AAA server. In this case, the local AAA needs to be configured. The local AAA does not support accounting.

Copyright © Huawei Technologies Co., Ltd.

- The MA5600T/MA5603T/MA5608T functions as the client of a remote AAA server, and is connected to the HWTACACS server through the HWTACACS protocol, implementing the AAA.
- The MA5600T/MA5603T/MA5608T functions as the client of a remote AAA server, and is connected to the RADIUS server through the RADIUS protocol, implementing the AAA. The RADIUS protocol, however, does not support authorization.

Table 2-2 lists the differences between HWTACACS and RADIUS.

Table 2-2 Differences between HWTACACS and RADIUS

HWTACACS	RADIUS
Uses TCP to ensure more reliable network transmission.	Uses UDP for transmission.
Encrypts the body of HWTACACS packets, except their header.	Encrypts only the password field of the authenticated packets.
Separated authorization and authentication.	Concurrent processing of authentication and authorization.
Applicable to security control.	Applicable to accounting.
Supports authorization of the configuration commands on the router.	Does not support the authorization of the configuration commands on the router.

2.4.1 Configuring the Local AAA

This topic describes how to configure the local AAA so that the user authentication can be performed locally.

Context

- The local AAA configuration is simple, which does not depend on the external server.
- The local AAA supports only authentication.

Procedure

Step 1 Configure the AAA authentication scheme.

NOTE

- The authentication scheme specifies how all the users in an Internet service provider (ISP) domain are authenticated. The system supports up to 16 authentication schemes.
- The system has a default authentication scheme named **default**. It can be modified, but cannot be deleted.

1. Run the **aaa** command to enter the AAA mode.
2. Run the **authentication-scheme** command to add an authentication scheme.
3. Run the **authentication-mode local** command to configure the authentication mode of the authentication scheme.

Copyright © Huawei Technologies Co., Ltd.

4. Run the **quit** command to return to the AAA mode.

Step 2 Create a domain.

NOTE

- A domain is a group of users of the same type.
- In the user name format userid@domain-name (for example, huawei20041028@huawei.net), "userid" indicates the user name for authentication and "domain-name" followed by "@" indicates the domain name.
- The domain name for user login cannot exceed 15 characters, and the other domain names cannot exceed 20 characters.

1. In the AAA mode, run the **domain** command to create a domain.

Step 3 Refer the authentication scheme.

NOTE

You can refer an authentication scheme in a domain only after the authentication scheme is created.

1. In the domain mode, run the **authentication-scheme** command to reference the authentication scheme.
2. Run the **quit** command to return to the AAA mode.

Step 4 Configure a local user.

In the AAA mode, run the **local-user** *username* **service-type** command to create a local AAA user.

----End

Example

User1 in the isp domain adopts the local server for authentication. The authentication scheme is newscheme, the password is a123456, do as follows:

```
huawei(config)#aaa
huawei(config-aaa)#authentication-scheme newscheme
  Info: Create a new authentication scheme
huawei(config-aaa-authen-newscheme)#authentication-mode local
huawei(config-aaa-authen-newscheme)#quit
huawei(config-aaa)#domain isp
  Info: Create a new domain
huawei(config-aaa-domain-isp)#authentication-scheme newscheme
huawei(config-aaa-domain-isp)#quit
huawei(config-aaa)#local-user user1@isp service-type terminal password a123456
```

2.4.2 Configuring the Remote AAA (RADIUS Protocol)

The MA5600T/MA5603T/MA5608T is interconnected with the RADIUS server through the RADIUS protocol to implement authentication and accounting.

Context

- What is RADIUS:
  - Radius is short for the remote authentication dial-in user service. It is a distributed information interaction protocol with the client-server structure. Generally, it is used to manage a large number of distributed dial-in users.

Copyright © Huawei Technologies Co., Ltd.

  - Radius implements the user accounting by managing a simple user authentication database.
  - The authentication and accounting requests of users can be passed on to the Radius server through a network access server (NAS).

- Principle of RADIUS:
  - When a user tries to access another network (or some network resources) by setting up a connection to the NAS through a network, the NAS forwards the user authentication and accounting information to the RADIUS server. The RADIUS protocol specifies the means of transmitting the user information and accounting information between the NAS and the RADIUS server.
  - The RADIUS server receives the connection requests of users sent from the NAS, authenticates the user account and password contained in the user authentication data, and returns the required data to the NAS.
- Specification:
  - For the MA5600T/MA5603T/MA5608T, the RADIUS is configured based on each RADIUS server group.
  - In actual networking, a RADIUS server group can be any of the following:
    - An independent RADIUS server
    - A pair of primary/secondary RADIUS servers with the same configuration but different IP addresses
  - The following lists the attributes of a RADIUS server template:
    - IP addresses of primary and secondary servers
    - Shared key
    - RADIUS server type
- The configuration of the RADIUS protocol defines only the essential parameters for the information exchange between the MA5600T/MA5603T/MA5608T and the RADIUS server. To make the essential parameters take effect, the RADIUS server group should be referenced in a certain domain.
- The RADIUS attribute list defines the attribute parameters for interaction between the MA5600T/MA5603T/MA5608T and the RADIUS server. **Table 2-3** describes the parameters.

Table 2-3 RADIUS attribute list

Parameter Code	Parameter Name	Description
1	User-Name	Indicates the user name for authentication.
2	Password	Indicates the user password for authentication. This parameter is valid only for PAP authentication.

Copyright © Huawei Technologies Co., Ltd.

Parameter Code	Parameter Name	Description
3	Challenge-Password	Indicates the user password for authentication. This parameter is valid only for CHAP authentication.
4	NAS-IP-Address	Indicates the IP address of the access device. If the RADIUS server group is bound to an interface address, use the bound interface address; otherwise, use the address of the interface where packets are sent.
5	NAS-Port	Indicates the user access port. The format of this parameter is four-digit slot ID + two-digit card number + five-digit port number + 21-digit VLAN ID.
6	Service-Type	Indicates the user service type. The value of this parameter is 2 (frame) for access users and is 6 for remote management users. Currently, the MA5600T/ MA5603T/MA5608T supports only 802.1x access users but not PPP, L2TP, or DHCP access users for RADIUS authentication.
7	Framed-Protocol	The value of this parameter is fixed to 1 (PPP) because ITU-T RFC 2856 does not define 802.1x for this parameter.
14	Login-IP-Host	Indicates the host IP address of a login user.
15	Login-Service	Indicates the login service type. The valid types are SSH, Rlogin, TCP Clear, PortMaster (proprietary), and LAT.

Copyright © Huawei Technologies Co., Ltd.

Parameter Code	Parameter Name	Description
24	State	If the access challenge packet that the RADIUS server sends to a device contains this parameter, the subsequent access request packet sent by the device to the RADIUS server must also contain this parameter of the same value as that is contained in the access challenge packet.
25	Class	If the access accept packet sent by the RADIUS server to a device contains this parameter, the subsequent charging request packet sent by the device to the RADIUS server must also contain this parameter of the same value. For a standard RADIUS server, a device can use the Class attribute to represent the CAR parameter.
27	Session-Timeout	Indicates the available remaining time in the unit of second. It is the user re-authentication time in the EAP challenge packet.
29	Termination-Action	Indicates the service termination mode. The valid modes are re-authentication and forcing users to go offline.
31	Calling-Station-Id	Allows the NAS to send the calling number.
32	NAS-Identifier	Indicates the host name of the device.
40	Acct-Status-Type	Indicates the charging packet type. ● 1: charging start packet ● 2: charging stop packet ● 3: real-time charging packet
41	Acct-Delay-Time	Indicates the time for generating a charging packet in the unit of second.

Copyright © Huawei Technologies Co., Ltd.

Parameter Code	Parameter Name	Description
42	Acct-Input-Octets	Indicates the number of upstream bytes in the unit of byte, kbyte, Mbyte, or Gbyte. The specific unit can be configured using commands.
43	Acct-Output-Octets	Indicates the number of downstream bytes in the unit of byte, kbyte, Mbyte, or Gbyte. The specific unit can be configured using commands.
44	Acct-Session-Id	Indicates the charging connection number. The connection numbers for the charging start packet, real-time charging packet, and charging stop packet of the same connection must be the same.
45	Acct-Authentic	Indicates the user authentication mode. ● 1: RADIUS authentication ● 2: local authentication
46	Acct-Session-Time	Indicates the time for a user to go online in the unit of second.
47	Acct-Input-Packets	Indicates the number of upstream packets.
48	Acct-Output-Packets	Indicates the number of downstream packets.
49	Terminate-Cause	Indicates the user connection interruption cause. The valid values are as follows: ● User-Request(1): The user actively goes offline. ● Lost Carrier(2): The handshake fails, such as the EAPOL detection fails. ● User Error(17): The user authentication fails or times out.

Copyright © Huawei Technologies Co., Ltd.

Parameter Code	Parameter Name	Description
52	Acct-Input-Gigawords	Indicates the number of upstream bytes in the unit of 4Gbyte, kbyte, Mbyte, or Gbyte. The specific unit can be configured using commands.
53	Acct-Output-Gigawords	Indicates the number of downstream bytes in the unit of 4Gbyte, kbyte, Mbyte, or Gbyte. The specific unit can be configured using commands.
55	Event-Timestamp	Indicates the user online time in the unit of second. The value is the absolute number of seconds counting from 1970-01-01 00:00:00.
60	CHAP-Challenge	Indicates the challenge field for CHAP authentication. This parameter is valid only for CHAP authentication.
61	NAS-Port-Type	Indicates the NAS port type.
79	EAP-Message	Carries EAP packets.
80	Message-Authenticator	Verifies validity of packets between the RADIUS server and RADIUS client to prevent malicious attacks.
85	Acct-Interim-Interval	Indicates the interval for real-time charging in the unit of second.
87	NAS-Port-Id	Indicates the user access port number. The format of this parameter uses the format when DHCP option 82 is in common raio mode.
88	Framed-Pool	Indicates the name and address segment number of the address pool. After being delivered by the RADIUS server, this parameter is filled to suboption 7 in user DHCP packets by the MA5600T/MA5603T/ MA5608T.

Copyright © Huawei Technologies Co., Ltd.

Parameter Code	Parameter Name	Description
26-29 **NOTE** The preceding parameters are RADIUS standard attributes. Starting from this row, the following parameters are Huawei-defined attributes.	Exec-Privilege	Indicates the priority of operation users such as SSH users. The value ranges from 0 to 15. ● 0: common user ● 1: operator ● 2: administrator ● 3-15: common user
26-60	Ip-Host-Address	Indicates the user IP address and MAC address that are contained in authentication and charging packets. The format is A.B.C.D HH:HH:HH:HH:HH:HH. The IP address and MAC address are separated by a space.
26-254	Version	Indicates the software version of the access device.
26-255	Product-ID	Indicates the product name.

NOTE

The super level user cannot be authenticated. You can query the user level by the command **display terminal user**.

Procedure

Step 1 Configure the authentication scheme.

NOTE

- The authentication scheme specifies how all the users in an ISP domain are authenticated.
- The system supports up to 16 authentication schemes. The system has a default accounting scheme named **default**. It can only be modified, but cannot be deleted.

1. Run the **aaa** command to enter the AAA mode.
2. Run the **authentication-scheme** command to add an authentication scheme.
3. Run the **authentication-mode radius** command to configure the authentication mode of the authentication scheme.
4. Run the **quit** command to return to the AAA mode.

Step 2 Configure the accounting scheme.

NOTE

- The accounting scheme specifies how all the users in an ISP domain are charged.
- The system supports up to 128 accounting schemes. The system has a default accounting scheme named **default**. It can be modified, but cannot be deleted.

Copyright © Huawei Technologies Co., Ltd.

1. In the AAA mode, run the **accounting-scheme** command to add an AAA accounting scheme.
2. Run the **accounting-mode radius** command to configure the accounting mode.
3. Run the **accounting interim interval** command to set the interval of real-time accounting. By default, the interval is 0 minutes, that is, the real-time accounting is not performed.
4. Run the **quit** command to return to the AAA mode.

Step 3 Configure the RADIUS server template.

1. Run the **radius-server template** command to create an RADIUS server template and enter the RADIUS server template mode.
2. Run the **radius-server authentication** command to configure the IP address and the UDP port ID of the RADIUS server for authentication.

   NOTE

   - To guarantee normal communication between the MA5600T/MA5603T/MA5608T and the RADIUS server, before configuring the IP address and UDP port of the RADIUS server, make sure that the route between the RADIUS server and the MA5600T/MA5603T/MA5608T is in the normal state.
   - Make sure that the configuration of the RADIUS service port of the MA5600T/MA5603T/MA5608T is consistent with the port configuration of the RADIUS server.
3. Run the **radius-server accounting** command to configure the IP address and the UDP port ID of the RADIUS server for accounting.
4. Run the **radius-server shared-key** command to configure the shared key of the RADIUS server.

   NOTE

   - The RADIUS client (MA5600T/MA5603T/MA5608T) and the RADIUS server use the MD5 algorithm to encrypt the RADIUS packets. They check the validity of the packets by setting the encryption key. They can receive the packets from each other and can respond to each other only when their keys are the same.
   - By default, the shared key of the RADIUS server is **huawei**.
5. (Optional) Run the **radius-server timeout** command to set the response timeout time of the RADIUS server. By default, the timeout time is 5s.

   The MA5600T/MA5603T/MA5608T sends the request packets to the RADIUS server. If the RADIUS server does not respond within the response timeout time, the MA5600T/MA5603T/MA5608T re-transmits the request packets to the RADIUS to ensure that users can get corresponding services from the RADIUS server.
6. (Optional) Run the **radius-server retransmit** command to set the maximum re-transmit time of the RADIUS request packets. By default, the maximum re-transmit time is 3.

   When the re-transmit time of the RADIUS request packets to a RADIUS server exceeds the maximum re-transmit time, the MA5600T/MA5603T/MA5608T considers that its communication with the RADIUS server is interrupted, and therefore transmits the RADIUS request packets to another RADIUS server.
7. Run the **(undo)radius-server user-name domain-included** command to configure the user name (not) to carry the domain name when transmitted to the RADIUS server. By default, the user name of the RADIUS server carries the domain name.

   - An access user is named in the format of **userid@domain-name**, and the part after @ is the domain name. The MA5600T/MA5603T/MA5608T classifies a user into a domain according to the domain name.

Copyright © Huawei Technologies Co., Ltd.

- If an RADIUS server group rejects the user name carrying the domain name, the RADIUS server group cannot be set or used in two or more domains. Otherwise, when some access users in different domains have the same user name, the RADIUS server considers that these users are the same because the names transmitted to the server are the same.

8. Run the **quit** command to return to the global config mode.

Step 4 Create a domain.

A domain is a group of users of the same type.

In the user name format userid@domain-name (for example, huawei20041028@huawei.net), "userid" indicates the user name for authentication and "domain-name" followed by "@" indicates the domain name.

The domain name for user login cannot exceed 15 characters, and the other domain names cannot exceed 20 characters.

1. Run the **aaa** command to enter the AAA mode.
2. In the AAA mode, run the **domain** command to create a domain.

Step 5 Use the authentication scheme.

You can use an authentication scheme in a domain only after the authentication scheme is created.

In the domain mode, run the **authentication-scheme** command to use the authentication scheme.

Step 6 Use the accounting scheme.

You can use an accounting scheme in a domain only after the accounting scheme is created.

In the domain mode, run the **accounting-scheme** command to use the accounting scheme.

Step 7 Use the RADIUS server template.

NOTE

You can use a RADIUS server template in a domain only after the RADIUS server template is created.

1. In the domain mode, run the **radius-server template** command to use the RADIUS server template.
2. Run the **quit** command to return to the AAA mode.

----End

Example

User1 in the isp domain adopts the HWTACACS protocol for authentication and accounting. The accounting interval is 10 minutes, the authentication password is a123456, HWTACACS server 10.10.66.66 functions as the primary authentication and accounting server, and HWTACACS server 10.10.66.67 functions as the standby authentication and accounting server. On the HWTACACS server, the authentication port ID is 1812, accounting port ID 1813, and other parameters adopt the default values. To perform the preceding configuration, do as follows:

```
huawei(config)#aaa
huawei(config-aaa)#authentication-scheme newscheme
huawei(config-aaa-authen-newscheme)#authentication-mode radius
```


Copyright © Huawei Technologies Co., Ltd.

```
huawei(config-aaa-authen-newscheme)#quit
huawei(config-aaa)#accounting-scheme newscheme
huawei(config-aaa-accounting-newscheme)#accounting-mode radius
huawei(config-aaa-accounting-newscheme)#accounting interim interval 10
huawei(config-aaa-accounting-newscheme)#quit
huawei(config)#radius-server template hwtest
huawei(config-radius-hwtest)#radius-server authentication 10.10.66.66 1812
huawei(config-radius-hwtest)#radius-server authentication 10.10.66.67 1812
secondary
huawei(config-radius-hwtest)#radius-server accounting 10.10.66.66 1813
huawei(config-radius-hwtest)#radius-server accounting 10.10.66.67 1813 secondary
huawei(config-radius-hwtest)#quit
huawei(config)#aaa
huawei(config-aaa)#domain isp
huawei(config-aaa-domain-isp)#authentication-scheme newscheme
huawei(config-aaa-domain-isp)#accounting-scheme newscheme
huawei(config-aaa-domain-isp)#radius-server hwtest
huawei(config-aaa-domain-isp)#quit
```

2.4.3 Configuration Example of the RADIUS Authentication and Accounting

The MA5600T/MA5603T/MA5608T is interconnected with the RADIUS server through the RADIUS protocol to implement authentication and accounting.

Service Requirements

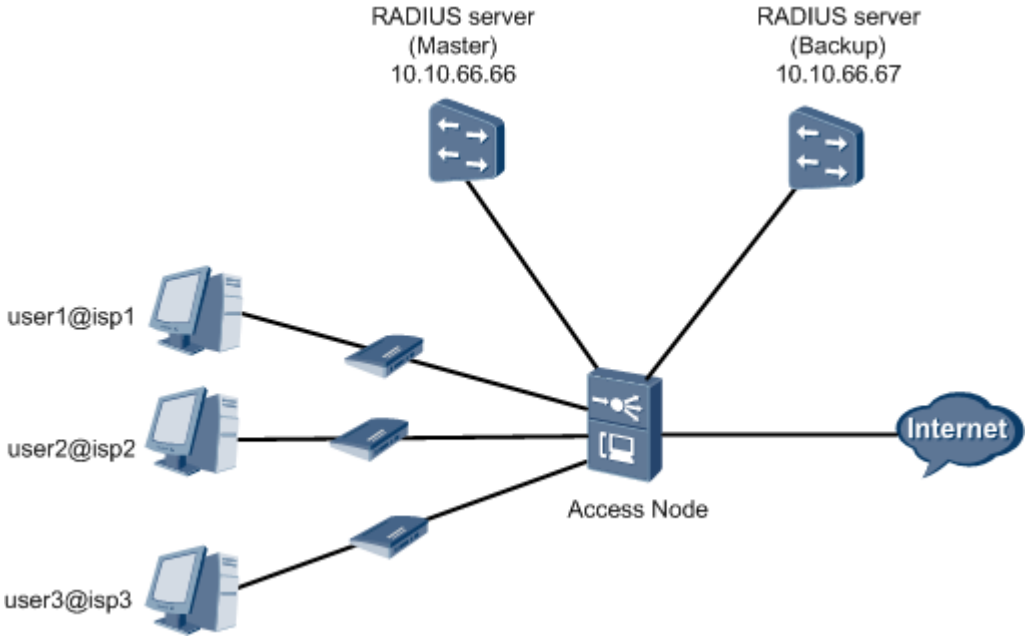
- The RADIUS server performs authentication and accounting for users in the ISP1 and ISP2 domains.
- The RADIUS server with the IP address 10.10.66.66 functions as the primary server for authentication and accounting.
- The RADIUS server with the IP address 10.10.66.67 functions as the secondary server for authentication and accounting.
- The authentication port number is 1812, and the accounting port number is 1813.
- Other parameters adopt the default settings.

Networking

Figure 2-2 shows an example network of the RADIUS Authentication and Accounting application.

Copyright © Huawei Technologies Co., Ltd.

Figure 2-2 Example network of the RADIUS Authentication and Accounting application.



Procedure

Step 1 Configure the authentication scheme.

Configure authentication scheme named **newscheme** (users are authenticated through RADIUS).

```
huawei(config)#aaa
huawei(config-aaa)#authentication-scheme newscheme
  Info: Create a new authentication scheme
huawei(config-aaa-authen-newscheme)#authentication-mode radius
huawei(config-aaa-authen-newscheme)#quit
```

Step 2 Configure the accounting scheme.

Configure accounting scheme named **newscheme** (users are authenticated through RADIUS). the interval is 10 minutes.

```
huawei(config-aaa)#accounting-scheme newscheme
  Info: Create a new accounting scheme
huawei(config-aaa-accounting-newscheme)#accounting-mode radius
huawei(config-aaa-accounting-newscheme)#accounting interim interval 10
huawei(config-aaa-accounting-newscheme)#quit
huawei(config-aaa)#quit
```

Step 3 Configure the RADIUS protocol.

Create RADIUS server template named **hwtest** with the RADIUS server 10.10.66.66 as the primary authentication and accounting server, and the RADIUS server 10.10.66.67 as the secondary authentication and accounting server.

```
huawei(config)#radius-server template hwtacacs
 Note: Create a new server template
huawei(config-radius-hwtacacs)#radius-server authentication 10.10.66.66 1812
huawei(config-radius-hwtacacs)#radius-server authentication 10.10.66.67 1812
```


Copyright © Huawei Technologies Co., Ltd.

```
secondary
huawei(config-radius-hwtacacs)#radius-server accounting 10.10.66.66 1813
huawei(config-radius-hwtacacs)#radius-server accounting 10.10.66.67 1813 secondary
huawei(config-radius-hwtacacs)#quit
```

Step 4 Create a domain.

Create a domain named isp1.

```
huawei(config)
#aaa
huawei(config-aaa)#domain isp1
  Info: Create a new domain
```

Step 5 Use the authentication scheme.

You can use an authentication scheme in a domain only after the authentication scheme is created.

```
huawei(config-aaa-domain-isp1)#authentication-scheme newscheme
```

Step 6 Use the accounting scheme.

You can use an accounting scheme in a domain only after the accounting scheme is created.

```
huawei(config-aaa-domain-isp1)#accounting-scheme newscheme
```

Step 7 Use the RADIUS server template.

You can use a RADIUS server template in a domain only after the RADIUS server template is created.

```
huawei(config-aaa-domain-isp1)#radius-server hwtacacs
huawei(config-aaa-domain-isp1)#quit
```

----End

Result

User 1 in ISP 1 can pass authentication only if both the user name and password are correct, and then can log in to the MA5600T/MA5603T/MA5608T. Then, the user starts to be accounted.

Configuration File

```
aaa
authentication-scheme newscheme
authentication-mode radius
quit
accounting-scheme
newscheme
accounting-mode
radius
accounting interim interval 10
quit
quit
radius-server template radtest
radius-server authentication 10.10.66.66
1812
radius-server authentication 10.10.66.67 1812 secondary
radius-server accounting 10.10.66.66
1813
radius-server accounting 10.10.66.67 1813 secondary
quit
```


Copyright © Huawei Technologies Co., Ltd.

```
aaa

domain
isp1
authentication-scheme newscheme
accounting-scheme newscheme
radius-server
hwtacacs
quit
```

2.4.4 Configuring the Remote AAA (HWTACACS Protocol)

The MA5600T/MA5603T/MA5608T is interconnected with the HWTACACS server through the HWTACACS protocol to implement authentication, authorization, and accounting.

Context

- What is HWTACACS:
  - HWTACACS is a security protocol with enhanced functions on the base of TACACS (RFC1492). Similar to the RADIUS protocol, HWTACACS implements multiple subscriber AAA functions through communications with the HWTACACS server in the client/server (C/S) mode.
  - HWTACACS is used for the authentication, authorization, and accounting for the 802.1 access users and management users.
- Principle of HWTACACS:

  Adopting the client/server architecture, HWTACACS is a protocol through which the NAS (MA5600T/MA5603T/MA5608T) transmits the encrypted HWTACACS data packets to communicate with the HWTACACS database of the security server. The working mode is as follows:
  - HWTACACS authentication. When the remote user connects to the corresponding port of the NAS, the NAS communicates with the daemon of the HWTACACS server, and obtains the prompt of entering the user name from the daemon. Then, the NAS displays the message to the user. When the remote user enters the user name, the NAS transmits the user name to the daemon. Then, the NAS obtains the prompt of entering the password, and displays the message to the user. After the remote user enters the password, the NAS transmits the password to the daemon.
  - HWTACACS authorization. After being authenticated, the user can be authorized. The NAS communicates with the daemon of the HWTACACS server, and then returns the accept or reject response of the authorization.

NOTE

- The HWTACACS configuration only defines the parameters used for data exchange between the MA5600T/MA5603T/MA5608T and the HWTACACS server. To make these parameters take effect, you need to use the HWTACACS server group in a domain.
- The settings of an HWTACACS server template can be modified regardless of whether the template is bound to a server or not.

Procedure

Step 1 Configure the AAA authentication scheme.

The authentication scheme specifies how all the users in an ISP domain are authenticated.

Copyright © Huawei Technologies Co., Ltd.

The system supports up to 16 authentication schemes. The system has a default authentication scheme named **default**. It can be modified, but cannot be deleted.

1. Run the **aaa** command to enter the AAA mode.
2. Run the **authentication-scheme** command to add an authentication scheme.
3. Run the **authentication-mode local** command to configure the authentication mode of the authentication scheme. Use the HWTACACS protocol to authenticate users.
4. Run the **quit** command to return to the AAA mode.

Step 2 Configure the AAA authorization scheme.

The authorization scheme specifies how all the users in an ISP domain are authorized.

1. In the AAA mode, run the **authorization-scheme** command to add an AAA authorization scheme.
2. Run the **authorization-mode hwtacacs** command to configure the authorization mode.
3. Run the **quit** command to return to the AAA mode.
4. Run the **quit** command to return to the global config mode.

Step 3 Configure the AAA accounting scheme.

The accounting scheme specifies how all the users in an ISP domain are charged.

The system supports up to 128 accounting schemes. The system has a default accounting scheme named **default**. It can be modified, but cannot be deleted.

1. In the AAA mode, run the **accounting-scheme** command to add an AAA accounting scheme.
2. Run the **accounting-mode hwtacacs** command to configure the accounting mode. By default, the accounting is not performed.
3. Run the **accounting interim interval** command to set the interval of real-time accounting. By default, the interval is 0 minutes, that is, the real-time accounting is not performed.
4. Run the **quit** command to return to the AAA mode.

Step 4 Configure the HWTACACS protocol.

The configuration of the HWTACACS protocol of the MA5600T/MA5603T/MA5608T is on the basis of the HWTACACS server group. In actual networking scenarios, an HWTACACS server group can be an independent HWTACACS server or a combination of two HWTACACS servers, that is, a primary server and a secondary server with the same configuration but different IP addresses.

Each HWTACACS server template contains the primary/secondary server IP address, shared key, and HWTACACS server type.

Primary and secondary authentication, accounting, and authorization servers can be configured. The IP address of the primary server, however, must be different from that of the secondary server. Otherwise, the configuration of primary and secondary servers will fail. By default, the IP addresses of the primary and secondary servers are both 0.0.0.0.

1. Run the **hwtacacs-server template** command to create an HWTACACS server template and enter the HWTACACS server template mode.
2. Run the **hwtacacs-server authentication** command to configure a primary authentication server. You can select **secondary** to configure a secondary authentication server.

Copyright © Huawei Technologies Co., Ltd.

NOTE

- To ensure normal communication between the MA5600T/MA5603T/MA5608T and the HWTACACS server, before configuring the IP address and the UDP port of the HWTACACS server, make sure that the route between the HWTACACS server and the MA5600T/MA5603T/MA5608T is in the normal state.
- Make sure that the HWTACACS server port of the MA5600T/MA5603T/MA5608T is the same as the port of the HWTACACS server.

3. Run the **hwtacacs-server accounting** command to configure a primary accounting server. You can select **secondary** to configure a secondary accounting server.
4. Run the **hwtacacs-server authorization** command to configure a primary authorization server. You can select **secondary** to configure a secondary authorization server.
5. (Optional) Run the **hwtacacs-server shared-key** command to configure the shared key of the HWTACACS server.

   NOTE

   - The HWTACACS client (MA5600T/MA5603T/MA5608T) and the HWTACACS server use the MD5 algorithm to encrypt the HWTACACS packets. They check the validity of the packets by configuring the encryption key. They can receive the packets from each other and can respond to each other only when their keys are the same.
   - By default, the HWTACACS server does not have a key.
6. (Optional) Run the **hwtacacs-server timer response-timeout** to set the response timeout time of the HWTACACS server.

   NOTE

   - If the HWTACACS server does not respond to the HWTACACS request packets within the timeout time, the communication between the MA5600T/MA5603T/MA5608T and the current HWTACACS server is considered as interrupted.
   - By default, the response timeout time of the HWTACACS server is 5s.
7. (Optional) In the global config mode, run the **hwtacacs-server accounting-stop-packet** command to configure the re-transmission mechanism of the accounting-stop packets of the HWTACACS server.

   NOTE

   - To prevent the loss of the accounting packets, the MA5600T/MA5603T/MA5608T supports the re-transmission of the accounting-stop packets of the HWTACACS server.
   - By default, the re-transmit time of the accounting-stop packets of the HWTACACS server is 100.
8. (Optional) Run the **(undo)hwtacacs-server user-name domain-included** command to configure the user name (not) to carry the domain name when transmitted to the HWTACACS server.
   - By default, the user name of the HWTACACS server carries the domain name.
   - After the **undo hwtacacs-server user-name domain-included** command is executed, the domain name is deleted from the user name when the client sends authentication and authorization requests to the HWTACACS server. The domain name in the user name of the accounting request is, however, reserved. This is to ensure that the users can be distinguished from each other in the accounting.
9. Run the **quit** command to return to the global config mode.

Step 5 Create a domain.

A domain is a group of users of the same type.

Copyright © Huawei Technologies Co., Ltd.

In the user name format userid@domain-name (for example, huawei20041028@huawei.net), "userid" indicates the user name for authentication and "domain-name" followed by "@" indicates the domain name.

The domain name for user login cannot exceed 15 characters, and the other domain names cannot exceed 20 characters.

1. Run the **aaa** command to enter the AAA mode.
2. In the AAA mode, run the **domain** command to create a domain.

Step 6 Use the authentication scheme.

You can use an authentication scheme in a domain only after the authentication scheme is created.

In the domain mode, run the **authentication-scheme** command to use the authentication scheme.

Step 7 Use the accounting scheme.

You can use an accounting scheme in a domain only after the accounting scheme is created.

In the domain mode, run the **accounting-scheme** command to use the accounting scheme.

Step 8 Use the authorization scheme.

You can use an authorization scheme in a domain only after the authorization scheme is created.

In the domain mode, run the **authorization-mode** command to use the authorization scheme.

Step 9 Use the HWTACACS server template.

You can use an HWTACACS server template in a domain only after the HWTACACS server template is created.

1. In the domain mode, run the **hwtacacs-server** command to use the HWTACACS server template.
2. Run the **quit** command to return to the AAA mode.

----End

Example

User1 in the isp domain adopts the HWTACACS protocol for authentication, authorization, and accounting. The accounting interval is 10 minutes, the authentication password is a123456, HWTACACS server 10.10.66.66 functions as the primary authentication, authorization, and accounting server, and HWTACACS server 10.10.66.67 functions as the standby authentication, authorization, and accounting server. On the HWTACACS server, the parameters adopt the default values. To perform the preceding configuration, do as follows:

```
huawei(config)#aaa
huawei(config-aaa)#authentication-scheme newscheme
huawei(config-aaa-authen-newscheme)#authentication-mode hwtacacs
huawei(config-aaa-authen-newscheme)#quit
huawei(config-aaa)#authorization-scheme newscheme
huawei(config-aaa-author-newscheme)#authorization-mode hwtacacs
huawei(config-aaa-author-newscheme)#quit
huawei(config-aaa)#accounting-scheme newscheme
huawei(config-aaa-accounting-newscheme)#accounting-mode hwtacacs
huawei(config-aaa-accounting-newscheme)#accounting interim interval 10
```


Copyright © Huawei Technologies Co., Ltd.

```
huawei(config-aaa-accounting-newscheme)#quit
huawei(config)#hwtacacs-server template hwtest
huawei(config-hwtacacs-hwtest)#hwtacacs-server authentication 10.10.66.66
huawei(config-hwtacacs-hwtest)#hwtacacs-server authentication 10.10.66.67
secondary
huawei(config-hwtacacs-hwtest)#hwtacacs-server authorization 10.10.66.66
huawei(config-hwtacacs-hwtest)#hwtacacs-server authorization 10.10.66.67 secondary
huawei(config-hwtacacs-hwtest)#hwtacacs-server accounting 10.10.66.66
huawei(config-hwtacacs-hwtest)#hwtacacs-server accounting 10.10.66.67 secondary
huawei(config-hwtacacs-hwtest)#quit
huawei(config)#aaa
huawei(config-aaa)#domain isp
huawei(config-aaa-domain-isp)#authentication-scheme newscheme
huawei(config-aaa-domain-isp)#authorization-scheme newscheme
huawei(config-aaa-domain-isp)#accounting-scheme newscheme
huawei(config-aaa-domain-isp)#hwtacacs-server hwtest
huawei(config-aaa-domain-isp)#quit
```

2.4.5 Configuration Example of the HWTACACS Authentication (802.1X access user)

The MA5600T/MA5603T/MA5608T is interconnected with the HWTACACS server through the HWTACACS protocol to implement authentication, authorization, and accounting.

Service Requirements

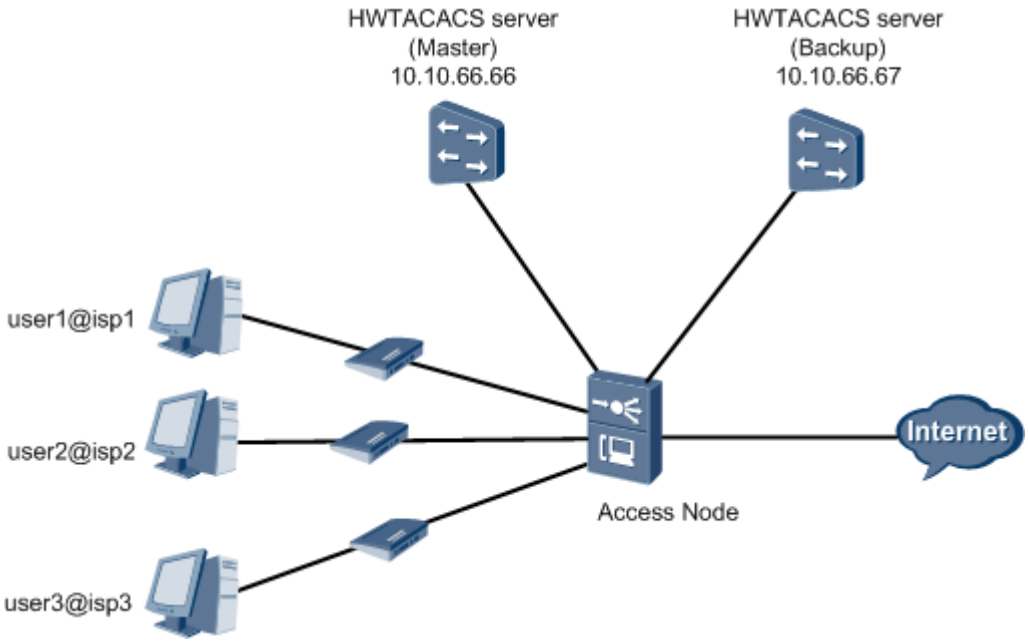
- The HWTACACS server performs authentication, authorization, and accounting for 802.1X access users.
- The user logs in to the server carrying the domain name.
- The HWTACACS server with the IP address 10.10.66.66 functions as the primary server for authentication, authorization, and accounting.
- The HWTACACS server with the IP address 10.10.66.67 functions as the secondary server for authentication, authorization, and accounting.
- Other parameters adopt the default settings.

Networking

Figure 2-3 shows an example network of the HWTACACS authentication.

Copyright © Huawei Technologies Co., Ltd.

Figure 2-3 Example network of the HWTACACS authentication



Procedure

Step 1 Configure an authentication scheme.

Configure authentication scheme named **newscheme** (users are authenticated through HWTACACS).

```
huawei(config)#aaa
huawei(config-aaa)#authentication-scheme newscheme
huawei(config-aaa-authen-newscheme)#authentication-mode hwtacacs
huawei(config-aaa-authen-newscheme)#quit
```

Step 2 Configure an authorization scheme.

Configure authorization scheme named **newscheme** (users are authorized through HWTACACS).

```
huawei(config-aaa)#authorization-scheme newscheme
huawei(config-aaa-author-newscheme)#authorization-mode hwtacacs
huawei(config-aaa-author-newscheme)#quit
```

Step 3 Configure the accounting scheme.

Configure accounting scheme named **newscheme** (users are authenticated through HWTACACS). the interval is 10 minutes.

```
huawei(config-aaa)#accounting-scheme newscheme
huawei(config-aaa-accounting-newscheme)#accounting-mode hwtacacs
huawei(config-aaa-accounting-newscheme)#accounting interim interval 10
huawei(config-aaa-accounting-newscheme)#quit
huawei(config-aaa)#quit
```

Step 4 Configure the HWTACACS protocol.

Copyright © Huawei Technologies Co., Ltd.

Create HWTACACS server template named **hwtest** with the HWTACACS server 10.10.66.66 as the primary authentication, authorization and accounting server, and the HWTACACS server 10.10.66.67 as the secondary authentication, authorization and accounting server.

```
huawei(config)#hwtacacs-server template hwtest
  Create a new HWTACACS-server template
huawei(config-hwtacacs-radtest)#hwtacacs-server authentication 10.10.66.66
huawei(config-hwtacacs-radtest)#hwtacacs-server authentication 10.10.66.67
secondary
huawei(config-hwtacacs-hwtest)#hwtacacs-server authorization 10.10.66.66
huawei(config-hwtacacs-hwtest)#hwtacacs-server authorization 10.10.66.67 secondary
huawei(config-hwtacacs-radtest)#hwtacacs-server accounting 10.10.66.66
huawei(config-hwtacacs-radtest)#hwtacacs-server accounting 10.10.66.67 secondary
huawei(config-hwtacacs-radtest)#quit
```

Step 5 Configure the 802.1X authentication.

1. Enable the 802.1X global switch. Enable the 802.1X authentication for ports 1, 2, and 3. The 802.1X needs to be triggered by DHCP. Therefore, the DHCP-trigger authentication must be enabled.

   ```
   huawei(config)#dot1x enable
   huawei(config)#dot1x service-port 1
   huawei(config)#dot1x service-port 2
   huawei(config)#dot1x service-port 3
   huawei(config)#dot1x dhcp-trigger enable
   ```

2. Configure an 802.1X parameters. In the local termination authentication, the 802.1X parameters should be configured to be in the EAP termination mode. The count of allowed handshake failure is 1 and the handshake interval is 20s.

   ```
   huawei(config)#dot1x keepalive retransmit 1 interval 20 service-port 1
   huawei(config)#dot1x keepalive retransmit 1 interval 20 service-port 2
   huawei(config)#dot1x keepalive retransmit 1 interval 20 service-port 3
   huawei(config)#dot1x eap-end service-port 1
   huawei(config)#dot1x eap-end service-port 2
   huawei(config)#dot1x eap-end service-port 3
   ```

Step 6 Create a domain.

Create a domain named isp1.

```
huawei(config)
#aaa
huawei(config-aaa)#domain isp1
  Info: Create a new domain
```

Step 7 Use the authentication scheme.

You can use an authentication scheme in a domain only after the authentication scheme is created.

```
huawei(config-aaa-domain-isp1)#authentication-scheme newscheme
```

Step 8 Use the authorization scheme.

You can use an authorization scheme in a domain only after the authorization scheme is created.

```
huawei(config-aaa-domain-isp1)#authorization-scheme newscheme
```

Step 9 Use the accounting scheme.

You can use an accounting scheme in a domain only after the accounting scheme is created.

```
huawei(config-aaa-domain-isp1)#accounting-scheme newscheme
```


Copyright © Huawei Technologies Co., Ltd.

Step 10 Bind the HWTACACS server template.

You can use an HWTACACS server template in a domain only after the HWTACACS server template is created.

```
huawei(config-aaa-domain-isp1)#hwtacacs-server hwtest
```

----End

Result

User 1 in ISP 1 can pass authentication only if both the user name and password are correct, and then can log in to the MA5600T/MA5603T/MA5608T. Then, the user starts to be accounted.

Configuration File

```
aaa
authentication-scheme newscheme
authentication-mode hwtacacs
quit
authorization-scheme newscheme
authorization-mode hwtacacs
quit
accounting-scheme newscheme
accounting-mode hwtacacs
accounting interim interval 10
quit
quit
hwtacacs-server template hwtest
hwtacacs-server authentication 10.10.66.66
hwtacacs-server authentication 10.10.66.67 secondary
hwtacacs-server authorization 10.10.66.66
hwtacacs-server authorization 10.10.66.67 secondary
hwtacacs-server accounting 10.10.66.66
hwtacacs-server accounting 10.10.66.67 secondary
quit
dot1x enable
dot1x service-port 1
dot1x service-port 2
dot1x service-port 3
dot1x dhcp-trigger enable
dot1x keepalive retransmit 1 interval 20 service-port 1
dot1x keepalive retransmit 1 interval 20 service-port 2
dot1x keepalive retransmit 1 interval 20 service-port 3
dot1x eap-end service-port 1
dot1x eap-end service-port 2
dot1x eap-end service-port 3


domain
isp1
authentication-scheme newscheme
authorization-scheme newscheme
accounting-scheme newscheme
hwtacacs-server hwtest
```

2.4.6 Configuration Example of HWTACACS Authentication (Management User)

The MA5600T/MA5603T/MA5608T allows the management user of the device to log in to the system by the HWTACACS authentication mode.

Copyright © Huawei Technologies Co., Ltd.

Prerequisites

- The route from the MA5600T/MA5603T/MA5608T to the HWTACACS server must be configured.
- The management user information (user name@domain and password) must be configured on the HWTACACS server.

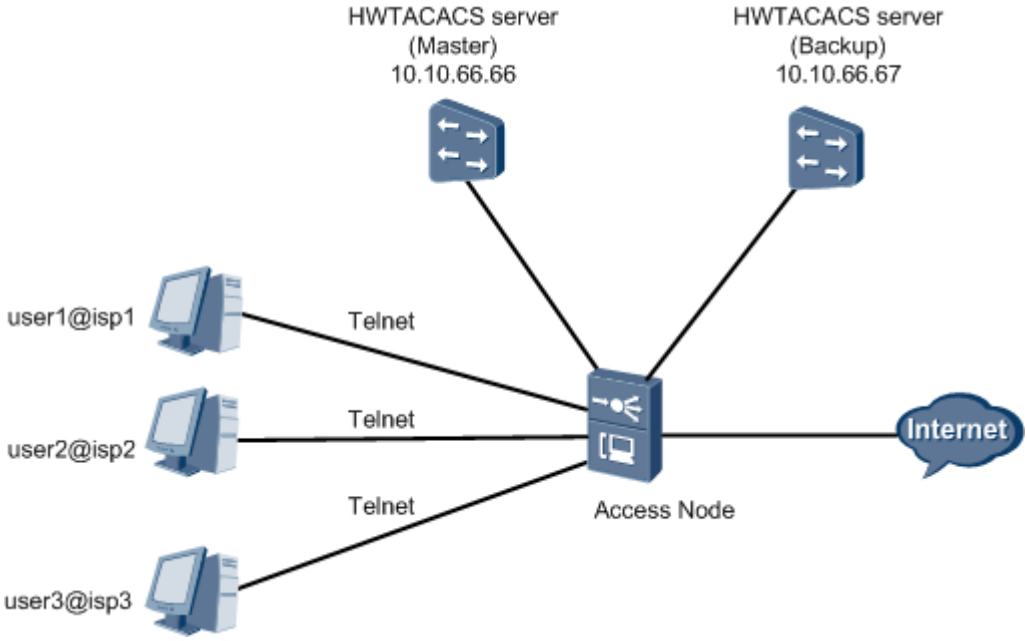
Service Requirements

- The HWTACACS server performs authentication for management user of domain **isp1**.
- The user logs in to the server carrying the domain name.
- The HWTACACS server with the IP address 10.10.66.66 functions as the primary server for authentication.
- The HWTACACS server with the IP address 10.10.66.67 functions as the secondary server for authentication.
- Other parameters adopt the default settings.

Networking

Figure 2-4 shows an example network of HWTACACS authentication.

Figure 2-4 Example network of HWTACACS authentication



Procedure

Step 1 Configure the authentication scheme.

Configure authentication scheme named **login-auth** (users are authenticated through HWTACACS).

Copyright © Huawei Technologies Co., Ltd.

```
huawei(config)#aaa
huawei(config-aaa)#authentication-scheme login-auth
huawei(config-aaa-authen-login-auth)#authentication-mode hwtacacs
huawei(config-aaa-authen-login-auth)#quit
```

Step 2 Configure the HWTACACS protocol.

Create HWTACACS server template named **ma56t-login** with HWTACACS server 10.10.66.66 as the primary authentication server, and HWTACACS server 10.10.66.67 as the secondary authentication server.

```
huawei(config)#hwtacacs-server template ma56t-login
  Create a new HWTACACS-server template
huawei(config-hwtacacs-ma56t-login)#hwtacacs-server authentication 10.10.66.66
1812
huawei(config-hwtacacs-ma56t-login)#hwtacacs-server authentication 10.10.66.67
1812 secondary
huawei(config-hwtacacs-ma56t-login)#quit
```

Step 3 Create a domain named **isp1**.

NOTE

- A domain is a group of users of the same type.
- In the user name format userid@domain-name (for example, huawei20041028@huawei.net), "userid" indicates the user name for authentication and "domain-name" followed by "@" indicates the domain name.
- The domain name for user login cannot exceed 15 characters, and the other domain names cannot exceed 20 characters.

```
huawei(config)#aaa
huawei(config-aaa)#domain isp1
  Info: Create a new domain
```

Step 4 Use the authentication scheme **login-auth**.

You can use an authentication scheme in a domain only after the authentication scheme is created.

```
huawei(config-aaa-domain-isp1)#authentication-scheme login-auth
```

Step 5 Bind the HWTACACS server template **ma56t-login** to the user.

You can use an HWTACACS server template in a domain only after the HWTACACS server template is created.

```
huawei(config-aaa-domain-isp1)#hwtacacs-server ma56t-login
```

----End

Result

- When the HWTACACS server is reachable, the management user can log in to the MA5600T/MA5603T/MA5608T through SSH. After entering the user name and password specified on the HWTACACS server, the management user can successfully log in to the MA5600T/MA5603T/MA5608T.
- When the HWTACACS server is unreachable, the management user cannot log in to the MA5600T/MA5603T/MA5608T through SSH by entering the user name and password specified on the HWTACACS server.

Configuration File

```
huawei(config)#aaa
huawei(config-aaa)#authentication-scheme login-auth
```


Copyright © Huawei Technologies Co., Ltd.

```
huawei(config-aaa-authen-login-auth)#authentication-mode hwtacacs
huawei(config-aaa-authen-login-auth)#quit
huawei(config-aaa)#quit
huawei(config)#hwtacacs-server template ma56t-login
huawei(config-hwtacacs-ma56t-login)#hwtacacs-server authentication 10.10.66.66
1812
huawei(config-hwtacacs-ma56t-login)#hwtacacs-server authentication 10.10.66.67
1812 secondary
huawei(config-hwtacacs-ma56t-login)#quit
huawei(config)#aaa
huawei(config-aaa)#domain isp1
huawei(config-aaa-domain-isp1)#authentication-scheme login-auth
huawei(config-aaa-domain-isp1)#hwtacacs-server ma56t-login
huawei(config-aaa-domain-isp1)#quit
huawei(config-aaa)#quit
```

2.5 Configuring DOCSIS Event Reporting

DOCSIS 3.0 defines various DOCSIS events, such as authentication failure and CM certificate error events. Configuring DOCSIS event reporting helps you obtain MA5600T/MA5603T/MA5608T and CM running status.

Procedure

Step 1 Run the **cable event loghost ip***ServerIpAddress* command to set the IP address of a log host to which DOCSIS events are reported.

Step 2 Run the **cable event level report** { **localVolatile** | **trap** | **syslog** } command to configure the mode and priority of reporting DOCSIS events.

The modes of reporting DOCSIS events include **localVolatile**, **trap**, and **syslog**.

- **localVolatile**: indicates that the DOCSIS events are saved to MA5600T/MA5603T/MA5608T local logs but not to the buffer. The MA5600T/MA5603T/MA5608T does not save the DOCSIS events and clears them after being reset. Configure the **localVolatile** mode before setting the mode of reporting DOCSIS events to **trap** or **syslog**.
- **trap**: reports DOCSIS events to a log host, which is generally the U2000, as traps. After setting this mode, run the **snmp-agent target-host trap-hostname** command to configure the log host.
- **syslog**: reports DOCSIS events to a log host as system logs, which are displayed after the log host software parses them.

The mode of reporting DOCSIS events varies depending on the priorities of the DOCSIS events.

- Default mode of reporting DOCSIS events with emergency or alert priorities: **localVolatile**
- Default mode of reporting DOCSIS events with critical, error, warning, or notice priorities: **trap**, **syslog**, and **localVolatile**
- Default mode of reporting DOCSIS events with information or debugging priorities: not reported

----End

Example

The following is an example of the configurations used to enable the CM management feature:

Copyright © Huawei Technologies Co., Ltd.

- Priority of DOCSIS events: alert
- Mode of reporting DOCSIS events to the U2000: **trap**
- Mode of reporting DOCSIS events to the log host: **syslog**
- IP address of the U2000: 10.10.10.10
- IP address of the log host: 10.10.20.10

```
huawei(config)#cable event alert report trap
huawei(config)#snmp-agent target-host trap-hostname huawei address 10.10.10.10
trap-paramsname docsis
huawei(config)#cable event alert report syslog
huawei(config)#cable event loghost ip 10.10.20.10
```


Copyright © Huawei Technologies Co., Ltd.

3 Configuring the DSLAM Services

About This Chapter

This topic describes how to configure the typical services such as Internet access, multicast, voice, and triple play services on the MA5600T/MA5603T/MA5608T.

3.1 Example: Configuring the xDSL Internet Access Service
This topic describes how to configure the xDSL Internet access service in the PPPoE, IPoE, PPPoA, IPoA and 802.1X modes.

3.2 Example: Configuring the xDSL Multicast Service
This topic describes how to configure the multicast video service.

3.3 Example: Configuring the VoIP Service
This topic describes how to configure the H.248-based, MGCP-based, and SIP-based VoIP services respectively.

3.4 Example: Configuring the Triple Play
This topic describes how to configure the Triple Play on the MA5600T/MA5603T/MA5608T.

Copyright © Huawei Technologies Co., Ltd.

3.1 Example: Configuring the xDSL Internet Access Service

This topic describes how to configure the xDSL Internet access service in the PPPoE, IPoE, PPPoA, IPoA and 802.1X modes.

3.1.1 Example: Configuring the xDSL Internet Access Service Through PPPoE Dialup

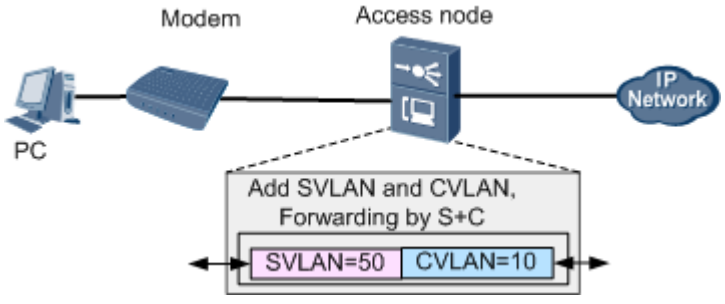
On a fiber to the x (FTTx) network, if the MA5600T/MA5603T/MA5608T provides x digital subscriber line (xDSL) services for broadband users and the users connect to the Internet in Point-to-Point Protocol over Ethernet (PPPoE) dialup mode, you can configure the MA5600T/MA5603T/MA5608T by referring to this topic to provide users with high-speed Internet (HIS) services. The MA5600T/MA5603T/MA5608T functions as an optical network unit (ONU) in this service. PPPoE is a commonly used Internet access mode currently. In this mode, broadband users are authenticated, authorized, and charged in Authentication, Authorization and Accounting (AAA) method.

Service Requirements

- The user accesses the Internet through the PPPoE dialup.
- The user packet goes upstream carrying two VLAN tags. The outer VLAN tag identifies the service and the inner VLAN tag identifies the user. The service of each user is identified by unique S-VLAN+C-VLAN, that is, this is a 1:1 access scenario.
- A traffic profile is adopted for rate limitation. The user access rate is 2048 kbit/s.
- To ensure reliability, dual GE ports are adopted for upstream transmission, and link aggregation is configured for the two upstream ports.

Figure 3-1 shows an example network of the xDSL Internet access service through the PPPoE dialup.

Figure 3-1 Example network of the xDSL Internet access service through the PPPoE dialup



Prerequisite

- The AAA function must be configured.
  - To enable the AAA function on the device, see **2.4 Configuring AAA**.

Copyright © Huawei Technologies Co., Ltd.

- If the AAA function is implemented by the BRAS, a connection to the BRAS must be established. The BRAS should be capable of identifying the VLAN tag of the MA5600T/MA5603T/MA5608T in the upstream direction. For the identification purpose, the user name and password for dial-up Internet access must be configured on the BRAS.

Procedure

Step 1 Configure a VLAN.

Configure S-VLAN 50 with the stacking attribute. The user packet goes upstream carrying two VLAN tags. The outer VLAN tag identifies the service and the inner VLAN tag identifies the user. The service of each user is identified by unique S-VLAN+C-VLAN, and the VLAN forwarding mode is the S-VLAN+C-VLAN mode.

```
huawei(config)#vlan 50 smart
huawei(config)#vlan attrib 50 stacking
huawei(config)#vlan forwarding 50 vlan-connect
```

Step 2 Configure upstream ports.

Add upstream ports 0/19/0 and 0/19/1 to VLAN 50. Two ports are added for the purpose of port aggregation.

```
huawei(config)#port vlan 50 0/19 0
huawei(config)#port vlan 50 0/19 1
```

To aggregate the two upstream ports as one aggregation group, set the packet forwarding mode of the aggregation group to egress-ingress, and set the aggregation group to work in the LACP static mode, do as follows:

```
huawei(config)#link-aggregation 0/19 0 0/19 1 egress-ingress workmode lacp-static
```

NOTE

The aggregated ports must meet the following requirements: The ports must work in the full-duplex mode; the port rates must be the same and the rate of an electrical port must not be of the auto-negotiation type; the attributes of the ports, such as the default VLAN ID (PVID) and VLAN, must be the same; one port can belong to only one aggregation group; the port must not be a mirroring destination port; the port must not be in the auto-negotiation mode; the start port ID must be smaller than the end port ID.

Step 3 In the ADSL access mode, follow this procedure.

1. Configure an ADSL2+ profile. For details, see Configuring ADSL2+ Profiles. The default ADSL2+ line template (line template 1) and the default ADSL2+ alarm template (alarm template 1) are used as an example.
2. Activate the ADSL port, and bind the ADSL2+ templates.

   NOTE

   By default, an ADSL port is in the activated state. Before binding a template to the port, you must deactivate the port.

   In the ADSL access mode, bind the default ADSL2+ line template 1 and ADSL2+ alarm template 1 to ADSL port 0/2/0.

   ```
   huawei(config)#interface adsl 0/2
   huawei(config-if-adsl-0/2)#deactivate 0
   huawei(config-if-adsl-0/2)#activate 0 profile-index 1
   huawei(config-if-adsl-0/2)#alarm-config 0 1
   huawei(config-if-adsl-0/2)#quit
   ```

3. Run the **display traffic table** command to query the existing traffic profiles in the system.

Copyright © Huawei Technologies Co., Ltd.

```
huawei(config)#display traffic table ip from-index 0
{ <cr>|to-index<K> }:

  Command:
          display traffic table ip from-index 0
  ------------------------------------------------------------------------------
   TID CIR       CBS       PIR       PBS       Pri Copy-policy         Pri-Policy
       (kbps)    (bytes)   (kbps)    (bytes)
  ------------------------------------------------------------------------------
     0 1024      34768     2048      69536      6 -                     tag-pri
     1 2496      81872     4992      163744     6 -                     tag-pri
     2 512       18384     1024      36768      0 -                     tag-pri
     3 576       20432     1152      40864      2 -                     tag-pri
     4 64        4048      128       8096       4 -                     tag-pri
     5 2048      67536     4096      135072     0 -                     tag-pri
     6 off       off       off       off        0 -                     tag-pri
  ------------------------------------------------------------------------------
  Total Num : 7
```

According to service requirements, the user access rate is 2048 kbit/s. The query result shows that traffic profile 5 (for inbound and outbound rate limitation) meets the requirements.

NOTE

- If a matched traffic profile is not available in the system, run the **traffic table ip** command to configure a new traffic profile.
- On the MA5600T/MA5603T/MA5608T, the user access rate can be limited by either a traffic profile or an ADSL line profile. When both profiles are configured, the smaller one of the two rates configured in the profiles is adopted as the user bandwidth. In this example, the traffic profile is used to limit the user access rate.

4. Run the **service-port** command to create a service port, adopt traffic profile 5, and set the S-VLAN ID to 50. The index of the service port is 1, and the VPI and VCI of the service port must be the same as the management VPI and VCI of the peer modem. Assume that the management VPI and VCI of the modem are 1 and 39, and the access port ID is 0/2/0. To facilitate the maintenance of the service port, also configure the service port description.

```
huawei(config)#service-port 1 vlan 50 adsl 0/2/0 vpi 1 vci 39 inbound traffic-
table index 5 outbound traffic-table index 5
huawei(config)#service-port desc 1 description Vlanid:50/adsl/vpi:1vci:39/
stacking
```

5. Set the C-VLAN ID of the preset service port 1 to 10 for identifying the user. Configure the important user packet with a higher priority so that the user packet can be processed with precedence, and set the priority of the inner VLAN to 4.

```
huawei(config)#stacking label service-port 1 10
huawei(config)#stacking inner-priority service-port 1 4
```

Step 4 In the SHDSL access mode, follow this procedure.

1. Configure an SHDSL profile. For details, see Configuring SHDSL Profiles. Add SHDSL line profile 3 of the PTM type, with the maximum line rate 2048 kbit/s.

```
huawei(config)#shdsl line-profile quickadd 3 ptm rate 512 2048
```

2. Activate SHDSL port 0/3/1, and bind the preset SHDSL line profile 3 and the default SHDSL alarm template (alarm template 1) to the port.

NOTE

By default, an SHDSL port is in the activated state. Before binding a profile or template to the port, you must deactivate the port.

```
huawei(config)#interface shl 0/3
huawei(config-if-shl-0/3)#deactivate 1
```


Copyright © Huawei Technologies Co., Ltd.

```
huawei(config-if-shl-0/3)#activate 1 3
huawei(config-if-shl-0/3)#alarm-config 1 1
huawei(config-if-shl-0/3)#quit
```

3. Run the **display traffic table** command to query the existing traffic profiles in the system.

```
huawei(config)#display traffic table ip from-index 0
{ <cr>|to-index<K> }:

  Command:
          display traffic table ip from-index 0
  ------------------------------------------------------------------------------
   TID CIR      CBS      PIR      PBS      Pri Copy-policy         Pri-Policy
       (kbps)   (bytes)  (kbps)   (bytes)
  ------------------------------------------------------------------------------
     0 1024     34768    2048     69536      6 -                     tag-pri
     1 2496     81872    4992     163744     6 -                     tag-pri
     2 512      18384    1024     36768      0 -                     tag-pri
     3 576      20432    1152     40864      2 -                     tag-pri
     4 64       4048     128      8096       4 -                     tag-pri
     5 2048     67536    4096     135072     0 -                     tag-pri
     6 off      off      off      off        0 -                     tag-pri
  ------------------------------------------------------------------------------
  Total Num : 7
```

According to service requirements, the user access rate is 2048 kbit/s. The query result shows that traffic profile 5 (for inbound and outbound rate limitation) meets the requirements.

NOTE

- If a matched traffic profile is not available in the system, run the **traffic table ip** command to configure a new traffic profile.
- On the MA5600T/MA5603T/MA5608T, the user access rate can be limited by either a traffic profile or an SHDSL line profile. When both profiles are configured, the smaller one of the two rates configured in the profiles is adopted as the user bandwidth. In this example, the traffic profile is used to limit the user access rate.

4. Run the **service-port** command to create a service port, adopt traffic profile 5, and set the S-VLAN ID to 50. Set the SHDSL channel mode to PTM, and create service port 2 on SHDSL port 0/3/1. To facilitate the maintenance of the service port, also configure the service port description.

```
huawei(config)#service-port 2 vlan 50 shdsl mode ptm 0/3/1 inbound traffic-
table
 index 5 outbound traffic-table index 5
huawei(config)#service-port desc 2 description Vlanid:50/shdsl/vpi:1vci:39/
stacking
```

5. Set the C-VLAN ID of the preset service port 2 to 10 for identifying the user. Configure the important user packet with a higher priority so that the user packet can be processed with precedence, and set the priority of the inner VLAN to 4.

```
huawei(config)#stacking label service-port 2 10
huawei(config)#stacking inner-priority service-port 2 4
```

Step 5 In the VDSL access mode, follow this procedure.

In this example, the VDSL normal mode is used as an example.

1. Configure a VDSL profile. For details, see Configuring VDSL2 Templates and Profiles. Assume that the VDSL profile ID is 3, downstream rate is 2048 kbit/s, channel mode is the interleave mode, maximum downstream interleave delay is 8 ms, maximum upstream interleave delay is 2 ms, SNR margin is 6 dB, minimum downstream INP is 4, and minimum upstream INP is 2.

Copyright © Huawei Technologies Co., Ltd.

```
huawei(config)#vdsl line-profile quickadd 3 snr 60 0 300 60 0 300
huawei(config)#vdsl channel-profile quickadd 3 path-mode ptm interleaved-delay
8 2 inp 4 2 rate
128 10000 128 10000 2048 2048
huawei(config)#vdsl line-template quickadd 3 line 3 channel1 3 100 100
```

2. Activate VDSL port 0/4/1, and bind the preset VDSL line template 3 and the default VDSL alarm template (alarm template 1) to the port.

   NOTE

   By default, a VDSL port is in the activated state. Before binding a template to the port, you must deactivate the port.

```
huawei(config)#interface vdsl 0/4
huawei(config-if-vdsl-0/4)#deactivate 1
huawei(config-if-vdsl-0/4)#activate 1 template-index 3
huawei(config-if-vdsl-0/4)#alarm-config 1 1
huawei(config-if-vdsl-0/4)#quit
```

3. Run the **display traffic table** command to query the existing traffic profiles in the system.

```
huawei(config)#display traffic table ip from-index 0
{ <cr>|to-index<K> }:

  Command:
          display traffic table ip from-index 0
  ------------------------------------------------------------------------------
   TID CIR      CBS      PIR      PBS      Pri Copy-policy         Pri-Policy
       (kbps)   (bytes)  (kbps)   (bytes)
  ------------------------------------------------------------------------------
     0 1024     34768    2048     69536      6 -                     tag-pri
     1 2496     81872    4992     163744     6 -                     tag-pri
     2 512      18384    1024     36768      0 -                     tag-pri
     3 576      20432    1152     40864      2 -                     tag-pri
     4 64       4048     128      8096       4 -                     tag-pri
     5 2048     67536    4096     135072     0 -                     tag-pri
     6 off      off      off      off        0 -                     tag-pri
  ------------------------------------------------------------------------------
  Total Num : 7
```

   According to service requirements, the user access rate is 2048 kbit/s. The query result shows that traffic profile 5 (for inbound and outbound rate limitation) meets the requirements.

   NOTE

   - If a matched traffic profile is not available in the system, run the **traffic table ip** command to configure a new traffic profile.
   - On the MA5600T/MA5603T/MA5608T, the user access rate can be limited by either a traffic profile or a VDSL line profile. When both profiles are configured, the smaller one of the two rates configured in the profiles is adopted as the user bandwidth. In this example, the traffic profile is used to limit the user access rate.

4. Run the **service-port** command to create a service port, adopt traffic profile 5, and set the S-VLAN ID to 50. Set the VDSL channel mode to PTM, and create service port 3 on VDSL port 0/4/1. To facilitate the maintenance of the service port, also configure the service port description.

```
huawei(config)#service-port 3 vlan 50 vdsl mode ptm 0/4/1 inbound traffic-
table
index 5 outbound traffic-table index 5
huawei(config)#service-port desc 3 description Vlanid:50/vdsl/vpi:1vci:39/
stacking
```

5. Set the C-VLAN ID of the preset service port 3 to 10 for identifying the user. Configure the important user packet with a higher priority so that the user packet can be processed with precedence, and set the priority of the inner VLAN to 4.

Copyright © Huawei Technologies Co., Ltd.

```
huawei(config)#stacking label service-port 3 10
huawei(config)#stacking inner-priority service-port 3 4
```

Step 6 Configure the user account security.

The PITP P mode can be enabled to protect the user account against theft and roaming. The RAIO mode can be customized according to actual requirements. The encoding format required by China Telecom is considered as an example. The encoding format required by China Telecom is a customized format, corresponding to the **cntel** option.

```
huawei(config)#pitp enable pmode
huawei(config)#raio-mode cntel pitp-pmode
```

NOTE

For details about the PITP configuration for the user account security, see Configuring Anti-theft and Roaming of User Accounts Using PITP.

Step 7 Save the data.

```
huawei(config)#save
```

----End

Verification

- Dialing verification on the user side:
  - Step 1: Configure the user name and password for the dialup on the modem (the user name and password must be the same as those configured on the BRAS).
  - Step 2: Dial up on the PC by using the PPPoE dialup software. After the dialup is successful, the user can access the Internet.
  - Step 3: When FTP is used to download files, after the dialup is performed on the PPPoE dialup software, the PPPoE dialup software prompts that the dialup is successful. Then, the PC can access the Internet in the PPPoE mode.
  - Step 4: When downloading files through FTP, you can open **Task Manager** in Windows and click **Networking** to check the link speed. Then, you can calculate the Internet access rate by the following formula: Attainable Internet access rate = Computer network adapter rate/48 x 53 x 8. The calculation result approximates to the planned 2048 kbit/s.
- Remote emulation dialing verification:
  - Step 1: On the MA5600T/MA5603T/MA5608T, run the **pppoe simulate start** command to start the PPPoE emulation dialer (the entered user name, password, and authentication mode must be the same as those configured on the BRAS).
  - Step 2: Run the **display pppoe simulate info** command to query status of PPPoE emulation dialing. If the PPPoE emulation dialing result is success, that is, simulating interaction between the user and the BRAS is successful, the user can access the Internet in the PPPoE access mode.
  - After the emulation verification is completed, run the **pppoe simulate stop** command to stop the PPPoE emulation dialing task initiated by the user.

Configuration File

Configuration File in the ADSL access mode:

```
vlan 50 smart
vlan attrib 50 stacking
```


Copyright © Huawei Technologies Co., Ltd.

```
vlan forwarding 50 vlan-connect
port vlan 50 0/19 0
port vlan 50 0/19 1
link-aggregation 0/19 0 0/19 1 egress-ingress workmode lacp-static
interface adsl 0/2
deactivate 0
activate 0 profile-index 1
alarm-config 0 1
quit
service-port 1 vlan 50 adsl 0/2/0 vpi 1 vci 39 inbound traffic-table index 5
outbound traffic-table index 5
service-port desc 1 description Vlanid:50/adsl/vpi:1vci:39/stacking
stacking label service-port 1 10
stacking inner-priority service-port 1 4
pitp enable pmode
raio-mode cntel pitp-pmode
save
```

Configuration File in the SHDSL access mode:

```
vlan 50 smart
vlan attrib 50 stacking
vlan forwarding 50 vlan-connect
port vlan 50 0/19 0
port vlan 50 0/19 1
link-aggregation 0/19 0 0/19 1 egress-ingress workmode lacp-static
shdsl line-profile quickadd 3 ptm rate 512 2048
interface shl 0/3
deactivate 1
activate 1 3
alarm-config 1 1
quit
service-port 2 vlan 50 shdsl mode ptm 0/3/1 inbound traffic-table index 5 outbound
traffic-table index 5
service-port desc 2 description Vlanid:50/shdsl/vpi:1vci:39/stacking
stacking label service-port 2 10
stacking inner-priority service-port 2 4
pitp enable pmode
raio-mode cntel pitp-pmode
save
```

Configuration File in the VDSL access mode:

```
vlan 50 smart
vlan attrib 50 stacking
vlan forwarding 50 vlan-connect
port vlan 50 0/19 0
port vlan 50 0/19 1
link-aggregation 0/19 0 0/19 1 egress-ingress workmode lacp-static
vdsl line-profile quickadd 3 snr 60 0 300 60 0 300
vdsl channel-profile quickadd 3 path-mode ptm interleaved-delay 8 2 inp 4 2 rate
128 10000 128 10000 2048 2048
interface vdsl 0/4
deactivate 1
activate 1 template-index 3
alarm-config 1 1
quit
service-port 3 vlan 50 vdsl mode ptm 0/4/1 inbound traffic-table index 5 outbound
traffic-table index 5
service-port desc 3 description Vlanid:50/vdsl/vpi:1vci:39/stacking
stacking label service-port 3 10
stacking inner-priority service-port 3 4
stacking inner-priority service-port 2 4
pitp enable pmode
raio-mode cntel pitp-pmode
save
```


Copyright © Huawei Technologies Co., Ltd.

3.1.2 Example: Configuring the xDSL IPoE Internet Access Service

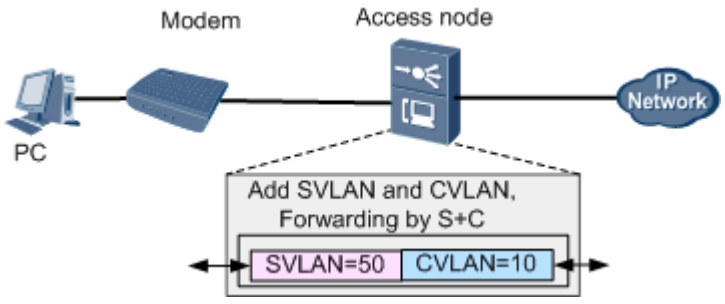
On a fiber to the x (FTTx) network, if the MA5600T/MA5603T/MA5608T provides x digital subscriber line (xDSL) services for broadband users and the users connect to the Internet in IP over Ethernet (IPoE) mode, you can configure the MA5600T/MA5603T/MA5608T by referring to this topic to provide users with high-speed Internet (HIS) services. The MA5600T/MA5603T/MA5608T functions as an optical network unit (ONU) in this service. IPoE is mainly used for private line IP access services. IPoE users are generally authenticated in Dynamic Host Configuration Protocol (DHCP) option 82 mode.

Service Requirements

- The OLT provides services for users in xDSL modes, including the asymmetric digital subscriber line 2 plus (ADSL2+), single-pair high-speed digital subscriber line (SHDSL), and very-high-speed digital subscriber line 2 (VDSL2) mode.
- Private line users connect to the Internet in IPoE mode. To prevent unauthorized access, user accounts are authenticated in DHCP option 82 mode.
- To trace service sources of users and control and manage quality of service (QoS) based on user and service, the Internet service is planned in per user per service per VLAN (PUPSPV) mode. To differentiate users, the MA5600T/MA5603T/MA5608T allocates a virtual local area network (VLAN) for each user. Double VLAN tags are added to user packets for upstream transmission, where the outer VLAN tag identifies the service and the inner VLAN tag identifies the user. The service of each user is identified by a unique S-VLAN+C-VLAN. This is called the 1:1 access.
- The user access rate is 2048 kbit/s.
- Dual GE ports are adopted for upstream transmission to ensure reliability. Link aggregation is configured for the two upstream ports.

Figure 3-2 shows an example network of the xDSL IPoE Internet access service.

Figure 3-2 Example network of the xDSL IPoE Internet access service



Prerequisite

The user PC can obtain an IP address from the DHCP server.

Procedure

Step 1 Configure a VLAN.

Copyright © Huawei Technologies Co., Ltd.

Configure S-VLAN 50 with the stacking attribute. The user packet goes upstream carrying two VLAN tags. The outer VLAN tag identifies the service and the inner VLAN tag identifies the user. The service of each user is identified by unique S-VLAN+C-VLAN, and the VLAN forwarding mode is the S-VLAN+C-VLAN mode.

```
huawei(config)#vlan 50 smart
huawei(config)#vlan attrib 50 stacking
huawei(config)#vlan forwarding 50 vlan-connect
```

Step 2 Configure upstream ports.

Add upstream ports 0/19/0 and 0/19/1 to VLAN 50. Two ports are added for the purpose of port aggregation.

```
huawei(config)#port vlan 50 0/19 0
huawei(config)#port vlan 50 0/19 1
```

To aggregate the two upstream ports as one aggregation group, set the packet forwarding mode of the aggregation group to egress-ingress, and set the aggregation group to work in the LACP static mode, do as follows:

```
huawei(config)#link-aggregation 0/19 0 0/19 1 egress-ingress workmode lacp-static
```

NOTE

The aggregated ports must meet the following requirements: The ports must work in the full-duplex mode; the port rates must be the same and the rate of an electrical port must not be of the auto-negotiation type; the attributes of the ports, such as the default VLAN ID (PVID) and VLAN, must be the same; one port can belong to only one aggregation group; the port must not be a mirroring destination port; the port must not be in the auto-negotiation mode; the start port ID must be smaller than the end port ID.

Step 3 In the ADSL access mode, follow this procedure.

1. Configure an ADSL2+ profile. For details, see Configuring ADSL2+ Profiles. The default ADSL2+ line template (line template 1) and the default ADSL2+ alarm template (alarm template 1) are used as an example.
2. Activate the ADSL port, and bind the ADSL2+ templates.

   NOTE

   By default, an ADSL port is in the activated state. Before binding a template to the port, you must deactivate the port.

   In the ADSL access mode, bind the default ADSL2+ line template 1 and ADSL2+ alarm template 1 to ADSL port 0/2/0.

   ```
   huawei(config)#interface adsl 0/2
   huawei(config-if-adsl-0/2)#deactivate 0
   huawei(config-if-adsl-0/2)#activate 0 profile-index 1
   huawei(config-if-adsl-0/2)#alarm-config 0 1
   huawei(config-if-adsl-0/2)#quit
   ```

3. Run the **display traffic table** command to query the existing traffic profiles in the system.

   ```
   huawei(config)#display traffic table ip from-index 0
   { <cr>|to-index<K> }:

     Command:
             display traffic table ip from-index 0
     ------------------------------------------------------------------------------
      TID CIR      CBS      PIR      PBS      Pri Copy-policy         Pri-Policy
          (kbps)   (bytes)  (kbps)   (bytes)
     ------------------------------------------------------------------------------
        0 1024     34768    2048     69536      6 -                   tag-pri
        1 2496     81872    4992     163744     6 -                   tag-pri
        2 512      18384    1024     36768      0 -                   tag-pri
        3 576      20432    1152     40864      2 -                   tag-pri
   ```


Copyright © Huawei Technologies Co., Ltd.

```
  4 64       4048     128      8096       4 -                        tag-pri
  5 2048     67536    4096     135072     0 -                        tag-pri
  6 off      off      off      off        0 -                        tag-pri
------------------------------------------------------------------------------
Total Num : 7
```

According to service requirements, the user access rate is 2048 kbit/s. The query result shows that traffic profile 5 (for inbound and outbound rate limitation) meets the requirements.

NOTE

- If a matched traffic profile is not available in the system, run the **traffic table ip** command to configure a new traffic profile.
- On the MA5600T/MA5603T/MA5608T, the user access rate can be limited by either a traffic profile or an ADSL line profile. When both profiles are configured, the smaller one of the two rates configured in the profiles is adopted as the user bandwidth. In this example, the traffic profile is used to limit the user access rate.

4. Run the **service-port** command to create a service port, adopt traffic profile 5, and set the S-VLAN ID to 50. The index of the service port is 1, and the VPI and VCI of the service port must be the same as the management VPI and VCI of the peer modem. Assume that the management VPI and VCI of the modem are 1 and 39, and the access port ID is 0/2/0. To facilitate the maintenance of the service port, also configure the service port description.

```
huawei(config)#service-port 1 vlan 50 adsl 0/2/0 vpi 1 vci 39 inbound traffic-
table index 5 outbound traffic-table index 5
huawei(config)#service-port desc 1 description Vlanid:50/adsl/vpi:1vci:39/
stacking
```

5. Set the C-VLAN ID of the preset service port 1 to 10 for identifying the user. Configure the important user packet with a higher priority so that the user packet can be processed with precedence, and set the priority of the inner VLAN to 4.

```
huawei(config)#stacking label service-port 1 10
huawei(config)#stacking inner-priority service-port 1 4
```

Step 4 In the SHDSL access mode, follow this procedure.

1. Configure an SHDSL profile. For details, see Configuring SHDSL Profiles. Add SHDSL line profile 3 of the PTM type, with the maximum line rate 2048 kbit/s.

```
huawei(config)#shdsl line-profile quickadd 3 ptm rate 512 2048
```

2. Activate SHDSL port 0/3/1, and bind the preset SHDSL line profile 3 and the default SHDSL alarm template (alarm template 1) to the port.

NOTE

By default, an SHDSL port is in the activated state. Before binding a profile or template to the port, you must deactivate the port.

```
huawei(config)#interface shl 0/3
huawei(config-if-shl-0/3)#deactivate 1
huawei(config-if-shl-0/3)#activate 1 3
huawei(config-if-shl-0/3)#alarm-config 1 1
huawei(config-if-shl-0/3)#quit
```

3. Run the **display traffic table** command to query the existing traffic profiles in the system.

```
huawei(config)#display traffic table ip from-index 0
{ <cr>|to-index<K> }:

  Command:
          display traffic table ip from-index 0
  ------------------------------------------------------------------------------
   TID CIR      CBS      PIR      PBS      Pri Copy-policy         Pri-Policy
```


Copyright © Huawei Technologies Co., Ltd.

```
     (kbps)   (bytes)  (kbps)   (bytes)
------------------------------------------------------------------------------
   0 1024     34768    2048     69536      6 -                        tag-pri
   1 2496     81872    4992     163744     6 -                        tag-pri
   2 512      18384    1024     36768      0 -                        tag-pri
   3 576      20432    1152     40864      2 -                        tag-pri
   4 64       4048     128      8096       4 -                        tag-pri
   5 2048     67536    4096     135072     0 -                        tag-pri
   6 off      off      off      off        0 -                        tag-pri
------------------------------------------------------------------------------
Total Num : 7
```

According to service requirements, the user access rate is 2048 kbit/s. The query result shows that traffic profile 5 (for inbound and outbound rate limitation) meets the requirements.

NOTE

- If a matched traffic profile is not available in the system, run the **traffic table ip** command to configure a new traffic profile.
- On the MA5600T/MA5603T/MA5608T, the user access rate can be limited by either a traffic profile or an SHDSL line profile. When both profiles are configured, the smaller one of the two rates configured in the profiles is adopted as the user bandwidth. In this example, the traffic profile is used to limit the user access rate.

4. Run the **service-port** command to create a service port, adopt traffic profile 5, and set the S-VLAN ID to 50. Set the SHDSL channel mode to PTM, and create service port 2 on SHDSL port 0/3/1. To facilitate the maintenance of the service port, also configure the service port description.

```
huawei(config)#service-port 2 vlan 50 shdsl mode ptm 0/3/1 inbound traffic-
table
 index 5 outbound traffic-table index 5
huawei(config)#service-port desc 2 description Vlanid:50/shdsl/vpi:1vci:39/
stacking
```

5. Set the C-VLAN ID of the preset service port 2 to 10 for identifying the user. Configure the important user packet with a higher priority so that the user packet can be processed with precedence, and set the priority of the inner VLAN to 4.

```
huawei(config)#stacking label service-port 2 10
huawei(config)#stacking inner-priority service-port 2 4
```

Step 5 In the VDSL access mode, follow this procedure.

In this example, the VDSL normal mode is used as an example.

1. Configure a VDSL profile. For details, see Configuring VDSL2 Templates and Profiles. Assume that the VDSL profile ID is 3, downstream rate is 2048 kbit/s, channel mode is the interleave mode, maximum downstream interleave delay is 8 ms, maximum upstream interleave delay is 2 ms, SNR margin is 6 dB, minimum downstream INP is 4, and minimum upstream INP is 2.

```
huawei(config)#vdsl line-profile quickadd 3 snr 60 0 300 60 0 300
huawei(config)#vdsl channel-profile quickadd 3 path-mode ptm interleaved-delay
8 2 inp 4 2 rate
128 10000 128 10000 2048 2048
huawei(config)#vdsl line-template quickadd 3 line 3 channel1 3 100 100
```

2. Activate VDSL port 0/4/1, and bind the preset VDSL line template 3 and the default VDSL alarm template (alarm template 1) to the port.

NOTE

By default, a VDSL port is in the activated state. Before binding a template to the port, you must deactivate the port.

Copyright © Huawei Technologies Co., Ltd.

```
huawei(config)#interface vdsl 0/4
huawei(config-if-vdsl-0/4)#deactivate 1
huawei(config-if-vdsl-0/4)#activate 1 template-index 3
huawei(config-if-vdsl-0/4)#alarm-config 1 1
huawei(config-if-vdsl-0/4)#quit
```

3. Run the **display traffic table** command to query the existing traffic profiles in the system.

```
huawei(config)#display traffic table ip from-index 0
{ <cr>|to-index<K> }:

  Command:
          display traffic table ip from-index 0
  ------------------------------------------------------------------------------
   TID CIR       CBS       PIR       PBS       Pri Copy-policy          Pri-Policy
       (kbps)    (bytes)   (kbps)    (bytes)
  ------------------------------------------------------------------------------
     0 1024      34768     2048      69536       6 -                      tag-pri
     1 2496      81872     4992      163744      6 -                      tag-pri
     2 512       18384     1024      36768       0 -                      tag-pri
     3 576       20432     1152      40864       2 -                      tag-pri
     4 64        4048      128       8096        4 -                      tag-pri
     5 2048      67536     4096      135072      0 -                      tag-pri
     6 off       off       off       off         0 -                      tag-pri
  ------------------------------------------------------------------------------
  Total Num : 7
```

According to service requirements, the user access rate is 2048 kbit/s. The query result shows that traffic profile 5 (for inbound and outbound rate limitation) meets the requirements.

NOTE

- If a matched traffic profile is not available in the system, run the **traffic table ip** command to configure a new traffic profile.
- On the MA5600T/MA5603T/MA5608T, the user access rate can be limited by either a traffic profile or a VDSL line profile. When both profiles are configured, the smaller one of the two rates configured in the profiles is adopted as the user bandwidth. In this example, the traffic profile is used to limit the user access rate.

4. Run the **service-port** command to create a service port, adopt traffic profile 5, and set the S-VLAN ID to 50. Set the VDSL channel mode to PTM, and create service port 3 on VDSL port 0/4/1. To facilitate the maintenance of the service port, also configure the service port description.

```
huawei(config)#service-port 3 vlan 50 vdsl mode ptm 0/4/1 inbound traffic-
table
index 5 outbound traffic-table index 5
huawei(config)#service-port desc 3 description Vlanid:50/vdsl/vpi:1vci:39/
stacking
```

5. Set the C-VLAN ID of the preset service port 3 to 10 for identifying the user. Configure the important user packet with a higher priority so that the user packet can be processed with precedence, and set the priority of the inner VLAN to 4.

```
huawei(config)#stacking label service-port 3 10
huawei(config)#stacking inner-priority service-port 3 4
```

Step 6 Configure the security of user accounts.

Copyright © Huawei Technologies Co., Ltd.

NOTE

- In this example, the MA5600T/MA5603T/MA5608T works in the Layer 2 DHCP mode. Therefore, the DHCP-related configurations are not required. If the MA5600T/MA5603T/MA5608T works in the Layer 3 DHCP mode, the DHCP-related configurations on the MA5600T/MA5603T/MA5608T are required. For details, see Configuring DHCP Relay.
- For the details about the security of DHCP accounts, see Configuring Anti-Theft and Roaming of DHCPv4 User Accounts Using DHCP Option 82.

Assume that the RAIO mode is the user-defined mode, the CID is the access node name frame/slot/port:vlanid, the RID is the label of the service port where the user is connected. To enable the DHCP option 82 function with these parameters, do as follows:

```
huawei(config)#dhcp option82 enable
huawei(config)#raio-mode user-defined dhcp-option82
huawei(config)#raio-format dhcp-option82 cid anid frame/slot/port:vlanid
huawei(config)#raio-format dhcp-option82 rid splabel
```

Step 7 Save the data.

```
huawei(config)#save
```

----End

Verification

- Internet access verification on the user side:
  - Step 1: After the PC NIC automatically obtains an IP address and a connection to the Internet is set up, the user can access the Internet.
  - Step 2: To download a file through FTP, open **Windows Task Manager** and then click **Networking** to observe the link rate. Calculate the Internet access rate by the formula: attainable Internet access rate = computer NIC rate/48 x 53 x 8. The calculated result approximates to the planned 2048 kbit/s.
- DHCP emulation verification:
  - Step 1: On the MA5600T/MA5603T/MA5608T run the **dhcp simulation start** command to start DHCP emulation.
  - Step 2: Run the **display dhcp simulation** command to query the DHCP emulation status.
  - After emulation is verified, run the **dhcp simulation stop** command to stop DHCP emulation.

Configuration File

Configuration File for the ADSL access mode:

```
vlan 50 smart
vlan attrib 50 stacking
vlan forwarding 50 vlan-connect
port vlan 50 0/19 0
port vlan 50 0/19 1
link-aggregation 0/19 0 0/19 1 egress-ingress workmode lacp-static
interface adsl 0/2
deactivate 0
activate 0 template-index 1
alarm-config 0 1
quit
service-port 1 vlan 50 adsl 0/2/0 vpi 1 vci 39 inbound traffic-table index 5
outbound traffic-table index 5
service-port desc 1 description Vlanid:50/adsl/vpi:1vci:39/stacking
```


Copyright © Huawei Technologies Co., Ltd.

```
stacking label service-port 1 10
stacking inner-priority service-port 1 4
dhcp option82 enable
raio-mode user-defined dhcp-option82
raio-format dhcp-option82 cid anid frame/slot/port:vlanid
raio-format dhcp-option82 rid splabel
save
```

Configuration File for the SHDSL access mode:

```
vlan 50 smart
vlan attrib 50 stacking
vlan forwarding 50 vlan-connect
port vlan 50 0/19 0
port vlan 50 0/19 1
link-aggregation 0/19 0 0/19 1 egress-ingress workmode lacp-static
shdsl line-profile quickadd 3 ptm rate 512 2048
interface shl 0/3
deactivate 1
activate 1 3
alarm-config 1 1
quit
service-port 2 vlan 50 shdsl mode ptm 0/3/1 inbound traffic-table index 5 outbound
traffic-table index 5
service-port desc 2 description Vlanid:50/shdsl/vpi:1vci:39/stacking
stacking label service-port 2 10
stacking inner-priority service-port 2 4
dhcp option82 enable
raio-mode user-defined dhcp-option82
raio-format dhcp-option82 cid anid frame/slot/port:vlanid
raio-format dhcp-option82 rid splabel
save
```

Configuration File for the VDSL access mode:

```
vlan 50 smart
vlan attrib 50 stacking
vlan forwarding 50 vlan-connect
port vlan 50 0/19 0
port vlan 50 0/19 1
link-aggregation 0/19 0 0/19 1 egress-ingress workmode lacp-static
vdsl line-profile quickadd 3 snr 60 0 300 60 0 300
vdsl channel-profile quickadd 3 path-mode ptm interleaved-delay 8 2 inp 4 2 rate
128 10000 128 10000 2048 2048
vdsl channel-profile quickadd 3 path-mode ptm interleaved-delay 8 2 inp 4 2 rate
128 10000 128 10000 2048 2048
interface vdsl 0/4
deactivate 0
activate 0 template-index 3
alarm-config 0 1
quit
service-port 3 vlan 50 vdsl mode ptm 0/4/1 inbound traffic-table index 5 outbound
traffic-table index 5
service-port desc 3 description Vlanid:50/vdsl/vpi:1vci:39/stacking
stacking label service-port 3 10
stacking inner-priority service-port 3 4
stacking inner-priority service-port 2 4
dhcp option82 enable
raio-mode user-defined dhcp-option82
raio-format dhcp-option82 cid anid frame/slot/port:vlanid
raio-format dhcp-option82 rid splabel
save
```


Copyright © Huawei Technologies Co., Ltd.

3.1.3 Example: Configuring the xDSL PPPoA Internet Access Service

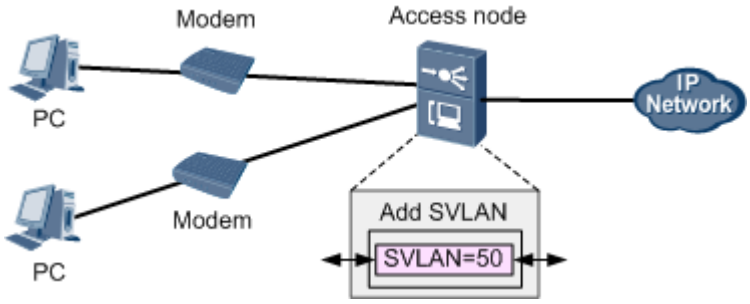
This topic describes how to configure a user so that the user can access the MA5600T/MA5603T/MA5608T in the xDSL mode, and then access the Internet in the PPPoA mode at a rate of 2048 kbit/s.

Service Requirements

- The user accesses the Internet in the PPPoA mode.
- User packets, which carry a single VLAN tag, are transmitted in the upstream direction, and the services of multiple users are converged into one VLAN. This is called the N:1 access.
- PITP is enabled to protect user accounts from theft and roaming.
- A traffic profile is adopted for rate limitation. The user access rate is 2048 kbit/s.
- Dual GE ports are adopted for upstream transmission to ensure reliability. Link aggregation is configured for the two upstream ports.

Figure 3-3 shows an example network of the xDSL PPPoA Internet access service.

Figure 3-3 Example network of the xDSL PPPoA Internet access service



Prerequisite

- The AAA function must be configured.
  - To enable the AAA function on the device, see **2.4 Configuring AAA**.
  - If the AAA function is implemented by the BRAS, a connection to the BRAS must be established. The BRAS should be capable of identifying the VLAN tag of the MA5600T/MA5603T/MA5608T in the upstream direction. For the identification purpose, the user name and password for dial-up Internet access must be configured on the BRAS.

Procedure

Step 1 Create a VLAN.

Create smart VLAN 50.

```
huawei(config)#vlan 50 smart
```


Copyright © Huawei Technologies Co., Ltd.

Step 2 Configure upstream ports.

Add upstream ports 0/19/0 and 0/19/1 to VLAN 50. Two ports are added for the purpose of port aggregation.

```
huawei(config)#port vlan 50 0/19 0
huawei(config)#port vlan 50 0/19 1
```

To aggregate the two upstream ports as one aggregation group, set the packet forwarding mode of the aggregation group to egress-ingress, and set the aggregation group to work in the LACP static mode, do as follows:

```
huawei(config)#link-aggregation 0/19 0 0/19 1 egress-ingress workmode lacp-static
```

NOTE

The aggregated ports must meet the following requirements: The ports must work in the full-duplex mode; the port rates must be the same and the rate of an electrical port must not be of the auto-negotiation type; the attributes of the ports, such as the default VLAN ID (PVID) and VLAN, must be the same; one port can belong to only one aggregation group; the port must not be a mirroring destination port; the port must not be in the auto-negotiation mode; the start port ID must be smaller than the end port ID.

Step 3 In the case of the ADSL access mode, follow this procedure.

1. Configure an ADSL2+ profile. For details, see **Configuring ADSL2+ Profiles**. The ID of the ADSL2+ line profile is 3, the downstream rate is 2048 kbit/s, the channel mode is the interleave mode, the maximum interleave delay is 10 ms, and the SNR margin is 6 dB.

```
huawei(config)#adsl line-profile quickadd 3 snr 60 30 120 60 30 120
huawei(config)#adsl channel-profile quickadd 3 interleaved-delay 10 10 rate
1024
 2048 3096 1024 2048
3096
huawei(config)#adsl line-template quickadd 3 line 3 channel1 3 60 70 channel2
3
```

2. Activate the ADSL port. The port is port 0/2/0, and ADSL line template 3 and the default alarm template (alarm template 1) are bound to the port.

   NOTE

   By default, an ADSL port is in the activated state. Before binding a template to the port, you must deactivate the port.

```
huawei(config)#interface adsl 0/2
huawei(config-if-adsl-0/2)#deactivate 0
huawei(config-if-adsl-0/2)#activate 0 template-index 3
huawei(config-if-adsl-0/2)#alarm-config 0 1
huawei(config-if-adsl-0/2)#quit
```

3. Run the **display traffic table ip** command to query the traffic profiles that exist in the system.

```
huawei(config)#display traffic table ip from-index 0
{ <cr>|to-index<K> }:

  Command:
          display traffic table ip from-index 0
  ------------------------------------------------------------------------------
   TID CIR      CBS      PIR      PBS      Pri Copy-policy         Pri-Policy
       (kbps)   (bytes)  (kbps)   (bytes)
  ------------------------------------------------------------------------------
     0 1024     34768    2048     69536      6 -                     tag-pri
     1 2496     81872    4992     163744     6 -                     tag-pri
     2 512      18384    1024     36768      0 -                     tag-pri
     3 576      20432    1152     40864      2 -                     tag-pri
     4 64       4048     128      8096       4 -                     tag-pri
     5 2048     67536    4096     135072     0 -                     tag-pri
     6 off      off      off      off        0 -                     tag-pri
  ------------------------------------------------------------------------------
  Total Num : 7
```


Copyright © Huawei Technologies Co., Ltd.

According to service requirement, the user access rate is 2048 kbit/s. The query result shows that traffic profile 5 meets the requirement.

NOTE

- If no traffic profile in the system meets the service requirement, run the **traffic table ip** command to configure a new traffic profile.
- On the MA5600T/MA5603T/MA5608T, the user access rate can be limited by either a traffic profile or an ADSL line profile. When both profiles are configured, the user bandwidth adopts the minimum value in the two profiles. In this example, the traffic profile is used to limit the user access rate.

4. Run the **service-port** command to create a service port. The index of the new service port is 1, the access port is port 0/2/0, traffic profile 5 meets the service requirement, and the S-VLAN is VLAN 50. The VPI and VCI must be the same as the management VPI and VCI of the peer modem. Assume that the management VPI and VCI of the modem are 1 and 39. To facilitate the maintenance of the service port, also configure the service port description.

```
huawei(config)#service-port 1 vlan 50 adsl 0/2/0 vpi 1 vci 39 inbound traffic-
table
 index 5 outbound traffic-table index 5
huawei(config)#service-port desc 1 description MA5600T/MA5603T/MA5608THW/
Vlanid:50/adsl/smart
```

5. Set the maximum number of MAC addresses that can be learned by the service port is 16. This parameter is to limit the maximum number of the MAC addresses that can be learned by one account, namely the maximum number of the PCs that can access the Internet through one account.

```
huawei(config)#mac-address max-mac-count service-port 1 16
```

Step 4 In the case of the SHDSL access mode, follow this procedure.

1. Configure an SHDSL profile. For details, see **Configuring SHDSL Profiles**. The ID of the SHDSL line profile is 3, the line rate is 2048 kbit/s, and the profile is used to activate 4-wire ports.

```
huawei(config)#shdsl line-profile quickadd 3 line four-wire rate 2048
```

2. Activate the SHDSL port. The port is port 0/3/1, and SHDSL line profile 3 and the default alarm profile (alarm profile 1) are bound to the port.

NOTE

By default, an ADSL port is in the activated state. Before binding a template to the port, you must deactivate the port.

```
huawei(config)#interface shl 0/3
huawei(config-if-shl-0/3)#deactivate 1
huawei(config-if-shl-0/3)#activate 1 3
huawei(config-if-shl-0/3)#alarm-config 1 1
huawei(config-if-shl-0/3)#quit
```

3. Run the **display traffic table ip** command to query the traffic profiles that exist in the system.

```
huawei(config)#display traffic table ip from-index 0
{ <cr>|to-index<K> }:

  Command:
          display traffic table ip from-index 0
  ------------------------------------------------------------------------------
   TID CIR      CBS      PIR      PBS      Pri Copy-policy         Pri-Policy
       (kbps)   (bytes)  (kbps)   (bytes)
  ------------------------------------------------------------------------------
     0 1024     34768    2048     69536      6 -                   tag-pri
     1 2496     81872    4992     163744     6 -                   tag-pri
     2 512      18384    1024     36768      0 -                   tag-pri
```


Copyright © Huawei Technologies Co., Ltd.

```
  3 576      20432    1152     40864      2 -                        tag-pri
  4 64       4048     128      8096       4 -                        tag-pri
  5 2048     67536    4096     135072     0 -                        tag-pri
  6 off      off      off      off        0 -                        tag-pri
-------------------------------------------------------------------------------
Total Num : 7
```

According to service requirement, the user access rate is 2048 kbit/s. The query result shows that traffic profile 5 meets the requirement.

NOTE

- If no traffic profile in the system meets the service requirement, run the **traffic table ip** command to configure a new traffic profile.
- On the MA5600T/MA5603T/MA5608T, the user access rate can be limited by either a traffic profile or an SHDSL line profile. When both profiles are configured, the user bandwidth adopts the minimum value in the two profiles. In this example, the traffic profile is used to limit the user access rate.

4. Run the **service-port** command to create a service port. The index of the new service virtual port is 2, the access port is port 0/3/1, traffic profile 5 meets the service requirement, and the S-VLAN is VLAN 50. The VPI and VCI must be the same as the management VPI and VCI of the peer modem. Assume that the management VPI and VCI of the modem are 1 and 39. To facilitate the maintenance of the service port, also configure the service port description.

```
huawei(config)#service-port 2 vlan 50 shdsl mode atm 0/3/1 vpi 1 vci 39 inbound
traffic-table
 index 5 outbound traffic-table index 5
huawei(config)#service-port desc 2 description MA5600T/MA5603T/MA5608THW/
Vlanid:50/shdsl/smart
```

5. Set the maximum number of MAC addresses that can be learned by the service port is 16. This parameter is to limit the maximum number of the MAC addresses that can be learned by one account, namely the maximum number of the PCs that can access the Internet through one account.

```
huawei(config)#mac-address max-mac-count service-port 2 16
```

Step 5 In the case of the VDSL access mode, follow this procedure.

In this example, the VDSL normal mode is used as an example.

1. Configure a VDSL profile. For details, see **Configuring VDSL2 Templates and Profiles**. Assume that the VDSL profile ID is 3, downstream rate is 2048 kbit/s, channel mode is the interleave mode, maximum downstream interleave delay is 8 ms, maximum upstream interleave delay is 2 ms, SNR margin is 6 dB, minimum downstream INP is 4, and minimum upstream INP is 2.

```
huawei(config)#vdsl line-profile quickadd 3 snr 60 0 300 60 0 300
huawei(config)#vdsl channel-profile quickadd 3 path-mode atm interleaved-delay
8 2 inp 4 2 rate
128 10000 128 10000 2048 2048
huawei(config)#vdsl line-template quickadd 3 line 3 channel1 3 100 100
```

2. Activate the VDSL port. The access port is port 0/4/1, and VDSL line template 3 and the default VDSL alarm template (alarm template 1) are bound to the port.

NOTE

By default, an ADSL port is in the activated state. Before binding a template to the port, you must deactivate the port.

```
huawei(config)#interface vdsl 0/4
huawei(config-if-vdsl-0/4)#deactivate 1
huawei(config-if-vdsl-0/4)#activate 1 template-index 3
```


Copyright © Huawei Technologies Co., Ltd.

```
huawei(config-if-vdsl-0/4)#alarm-config 1 1
huawei(config-if-vdsl-0/4)#quit
```

3. Run the **display traffic table ip** command to query the traffic profiles that exist in the system.

```
huawei(config)#display traffic table ip from-index 0
{ <cr>|to-index<K> }:

  Command:
          display traffic table ip from-index 0
  ------------------------------------------------------------------------------
   TID CIR      CBS      PIR      PBS      Pri Copy-policy         Pri-Policy
       (kbps)   (bytes)  (kbps)   (bytes)
  ------------------------------------------------------------------------------
     0 1024     34768    2048     69536      6 -                     tag-pri
     1 2496     81872    4992     163744     6 -                     tag-pri
     2 512      18384    1024     36768      0 -                     tag-pri
     3 576      20432    1152     40864      2 -                     tag-pri
     4 64       4048     128      8096       4 -                     tag-pri
     5 2048     67536    4096     135072     0 -                     tag-pri
     6 off      off      off      off        0 -                     tag-pri
  ------------------------------------------------------------------------------
  Total Num : 7
```

According to service requirement, the user access rate is 2048 kbit/s. The query result shows that traffic profile 5 meets the requirement.

NOTE

- If no traffic profile in the system meets the service requirement, run the **traffic table ip** command to configure a new traffic profile.
- On the MA5600T/MA5603T/MA5608T, the user access rate can be limited by either a traffic profile or a VDSL line profile. When both profiles are configured, the user bandwidth adopts the minimum value in the two profiles. In this example, the traffic profile is used to limit the user access rate.

4. Run the **service-port** command to create a service port. The index of the new service virtual port is 3, the access port is port 0/4/1, traffic profile 5 meets the service requirement, and the S-VLAN is VLAN 50. The VPI and VCI must be the same as the management VPI and VCI of the peer modem. Assume that the management VPI and VCI of the modem are 1 and 39. To facilitate the maintenance of the service port, also configure the service port description.

```
huawei(config)#service-port 3 vlan 50 vdsl mode atm 0/4/1 vpi 1 vci 39 inbound
traffic-table index 5 outbound
 traffic-table index 5
huawei(config)#service-port desc 3 description MA5600T/MA5603T/MA5608THW/
Vlanid:50/vdsl/smart
```

5. Set the maximum number of MAC addresses that can be learned by the service port is 16. This parameter is to limit the maximum number of the MAC addresses that can be learned by one account, namely the maximum number of the PCs that can access the Internet through one account.

```
huawei(config)#mac-address max-mac-count service-port 3 16
```

Step 6 Configure the PPPoA-PPPoE protocol conversion.

This step is to configure the PPPoA MAC address pool. The start MAC address in the MAC address pool is 0000-1111-1010, and the maximum number of the MAC addresses in the MAC address pool is 300. The PPPoA-PPPoE protocol conversion is enabled and the service encapsulation mode is LLC.

```
huawei(config)#mac-pool xpoa 0000-1111-1010 300
huawei(config)#pppoa enable
huawei(config)#encapsulation 0/2/0 vpi 1 vci 39 type pppoa llc
```


Copyright © Huawei Technologies Co., Ltd.

```
huawei(config)#encapsulation 0/3/1 vpi 1 vci 39 type pppoa llc
huawei(config)#encapsulation 0/4/1 vpi 1 vci 39 type pppoa llc
```

Step 7 Configure the user account security.

The PITP P mode can be enabled to protect the user account against theft and roaming. The RAIO mode can be customized according to actual requirements. The encoding format required by China Telecom is considered as an example. The encoding format required by China Telecom is a customized format, corresponding to the **cntel** option.

```
huawei(config)#pitp enable pmode
huawei(config)#raio-mode cntel pitp-pmode
```

NOTE

For details about the PITP configuration for the user account security, see Configuring Anti-theft and Roaming of User Accounts Using PITP.

Step 8 Save the data.

```
huawei(config)#save
```

----End

Verification

- Step 1: Set the VPI/VCI of the modem to 1/39 and encapsulation mode to **llc-pppoa**. Configure the user name and password used for dialing (the user name and password must be the same as those configured on the BRAS.)
- Step 2: After the settings on the modem are completed, dialing is initialized, a network connection is automatically set up, and the user can access the Internet.
- Step 3: To download a file through FTP, open **Windows Task Manager** and then click **Networking** to observe the link rate. Calculate the Internet access rate by the formula: attainable Internet access rate = computer NIC rate/48 x 53 x 8. The calculated result approximates to the planned 2048 kbit/s.

Configuration File

Configuration File for the ADSL access mode:

```
vlan 50 smart
port vlan 50 0/19 0
port vlan 50 0/19 1
link-aggregation 0/19 0 0/19 1 egress-ingress workmode lacp-static
adsl line-profile quickadd 3 2 snr 60 30 120 60 30 120
adsl channel-profile quickadd 3 interleaved-delay 10 10 rate 1024 2048 3096 1024
2048 3096
adsl line-template quickadd 3 line 3 channel1 3 60 70 channel2 3
interface adsl 0/2
deactivate 0
activate 0 template-index 3
alarm-config 0 1
quit
service-port 1 vlan 50 adsl 0/2/0 vpi 1 vci 39 inbound traffic-table index 5
outbound traffic-table index 5
service-port desc 1 description MA5600T/MA5603T/MA5608THW/Vlanid:50/adsl/smart
mac-address max-mac-count service-port 1 16
mac-pool xpoa 0000-1111-1010 300
pppoa enable
encapsulation 0/2/0 vpi 1 vci 39 type pppoa llc
pitp enable pmode
raio-mode cntel pitp-pmode
save
```


Copyright © Huawei Technologies Co., Ltd.

Configuration File for the SHDSL access mode:

```
vlan 50 smart
port vlan 50 0/19 0
port vlan 50 0/19 1
link-aggregation 0/19 0 0/19 1 egress-ingress workmode lacp-static
shdsl line-profile quickadd 3 line four-wire rate 2048
interface shl 0/3
deactivate 1
activate 1 3
alarm-config 1 1
quit
service-port 2 vlan 50 shdsl mode atm 0/3/1 vpi 1 vci 39 inbound traffic-table index
5 outbound traffic-table index 5
service-port desc 2 description MA5600T/MA5603T/MA5608THW/Vlanid:50/shdsl/smart
mac-address max-mac-count service-port 2 16
mac-pool xpoa 0000-1111-1010 300
pppoa enable
encapsulation 0/3/1 vpi 1 vci 39 type pppoa llc
pitp enable pmode
raio-mode cntel pitp-pmode
save
```

Configuration File for the VDSL access mode:

```
vlan 50 smart
port vlan 50 0/19 0
port vlan 50 0/19 1
link-aggregation 0/19 0 0/19 1 egress-ingress workmode lacp-static
vdsl line-profile quickadd 3 snr 60 0 300 60 0 300
vdsl channel-profile quickadd 3 path-mode atm interleaved-delay 8 2 inp 4 2 rate
128 10000 128 10000 2048 2048
interface vdsl 0/4
deactivate 1
activate 1 template-index 3
alarm-config 1 1
quit
service-port 3 vlan 50 vdsl mode atm 0/4/1 vpi 1 vci 39  inbound traffic-table index
5 outbound traffic-table index 5
service-port desc 3 description MA5600T/MA5603T/MA5608THW/Vlanid:50/vdsl/smart
mac-address max-mac-count service-port 3 16
mac-pool xpoa 0000-1111-1010 300
pppoa enable
encapsulation 0/4/1 vpi 1 vci 39 type pppoa llc
pitp enable pmode
raio-mode cntel pitp-pmode
save
```

3.1.4 Example: Configuring the xDSL IPoA Internet Access Service

On a fiber to the x (FTTx) network, if the MA5600T/MA5603T/MA5608T provides x digital subscriber line (xDSL) services for broadband users and the users connect to the Internet in IP over ATM (IPoA) mode, you can configure the MA5600T/MA5603T/MA5608T by referring to this topic to provide users with high-speed Internet (HIS) services. The MA5600T/MA5603T/MA5608T functions as an optical network unit in this service. IPoA is generally used on a private line network to meet operators' requirements for transferring from an asynchronous transfer mode (ATM) network to the IP network. An authentication is generally not required for IPoA users.

Service Requirements

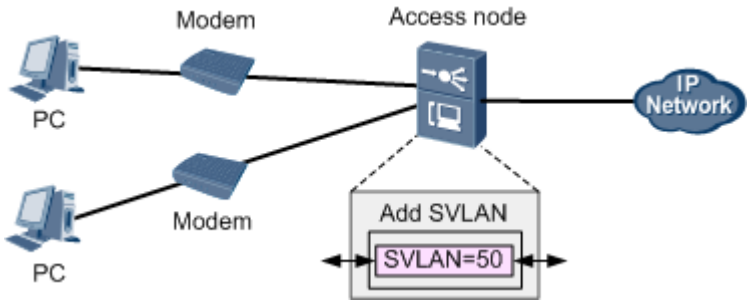
- The user accesses the Internet in the IPoA mode.

Copyright © Huawei Technologies Co., Ltd.

- To trace service sources of users and control and manage quality of service (QoS) based on user and service, the Internet service is planned in per user per service per VLAN (PUPSPV) mode. To differentiate users, the MA5600T/MA5603T/MA5608T allocates a virtual local area network (VLAN) for each user. On the OLT, use dual VLANs (S-VLAN +C-VLAN) to differentiate users for the Internet access service.
- The user access rate is 2048 kbit/s.
- Dual GE ports are adopted for upstream transmission to ensure reliability. Link aggregation is configured for the two upstream ports.

Figure 3-4 shows an example network of the xDSL IPoA Internet access service.

Figure 3-4 Example network of the xDSL IPoA Internet access service



Procedure

Step 1 Create a VLAN.

Create smart VLAN 50.

```
huawei(config)#vlan 50 smart
```

Step 2 Configure upstream ports.

Add upstream ports 0/19/0 and 0/19/1 to VLAN 50. Two ports are added for the purpose of port aggregation.

```
huawei(config)#port vlan 50 0/19 0
huawei(config)#port vlan 50 0/19 1
```

To aggregate the two upstream ports as one aggregation group, set the packet forwarding mode of the aggregation group to egress-ingress, and set the aggregation group to work in the LACP static mode, do as follows:

```
huawei(config)#link-aggregation 0/19 0 0/19 1 egress-ingress workmode lacp-static
```

NOTE

The aggregated ports must meet the following requirements: The ports must work in the full-duplex mode; the port rates must be the same and the rate of an electrical port must not be of the auto-negotiation type; the attributes of the ports, such as the default VLAN ID (PVID) and VLAN, must be the same; one port can belong to only one aggregation group; the port must not be a mirroring destination port; the port must not be in the auto-negotiation mode; the start port ID must be smaller than the end port ID.

Step 3 In the case of the ADSL access mode, follow this procedure.

1. Configure an ADSL2+ profile. For details, see **Configuring ADSL2+ Profiles**. The ID of the ADSL2+ line profile is 3, the downstream rate is 2048 kbit/s, the channel mode is the interleave mode, the maximum interleave delay is 10 ms, and the SNR margin is 6 dB.

Copyright © Huawei Technologies Co., Ltd.

```
huawei(config)#adsl line-profile quickadd 3 snr 60 30 120 60 30 120
huawei(config)#adsl channel-profile quickadd 3 interleaved-delay 10 10 rate
1024
 2048 3096 1024 2048
3096
huawei(config)#adsl line-template quickadd 3 line 3 channel1 3 60 70 channel2
3
```

2. Activate the ADSL port. The port is port 0/2/0, and ADSL line template 3 and the default alarm template (alarm template 1) are bound to the port.

   NOTE

   By default, an ADSL port is in the activated state. Before binding a template to the port, you must deactivate the port.

```
huawei(config)#interface adsl 0/2
huawei(config-if-adsl-0/2)#deactivate 0
huawei(config-if-adsl-0/2)#activate 0 template-index 3
huawei(config-if-adsl-0/2)#alarm-config 0 1
huawei(config-if-adsl-0/2)#quit
```

3. Run the **display traffic table ip** command to query the traffic profiles that exist in the system.

```
huawei(config)#display traffic table ip from-index 0
{ <cr>|to-index<K> }:

  Command:
          display traffic table ip from-index 0
  ------------------------------------------------------------------------------
   TID CIR      CBS      PIR      PBS      Pri Copy-policy         Pri-Policy
       (kbps)   (bytes)  (kbps)   (bytes)
  ------------------------------------------------------------------------------
     0 1024     34768    2048     69536      6 -                     tag-pri
     1 2496     81872    4992     163744     6 -                     tag-pri
     2 512      18384    1024     36768      0 -                     tag-pri
     3 576      20432    1152     40864      2 -                     tag-pri
     4 64       4048     128      8096       4 -                     tag-pri
     5 2048     67536    4096     135072     0 -                     tag-pri
     6 off      off      off      off        0 -                     tag-pri
  ------------------------------------------------------------------------------
  Total Num : 7
```

   According to service requirement, the user access rate is 2048 kbit/s. The query result shows that traffic profile 5 meets the requirement.

   NOTE

   - If no traffic profile in the system meets the service requirement, run the **traffic table ip** command to configure a new traffic profile.
   - On the MA5600T/MA5603T/MA5608T, the user access rate can be limited by either a traffic profile or an ADSL line profile. When both profiles are configured, the user bandwidth adopts the minimum value in the two profiles. In this example, the traffic profile is used to limit the user access rate.

4. Run the **service-port** command to create a service port. The index of the new service port is 1, the access port is port 0/2/0, traffic profile 5 meets the service requirement, and the S-VLAN is VLAN 50. The VPI and VCI must be the same as the management VPI and VCI of the peer modem. Assume that the management VPI and VCI of the modem are 1 and 39. To facilitate the maintenance of the service port, also configure the service port description.

```
huawei(config)#service-port 1 vlan 50 adsl 0/2/0 vpi 1 vci 39 inbound traffic-
table
 index 5 outbound traffic-table index 5
huawei(config)#service-port desc 1 description MA5600T/MA5603T/MA5608THW/
Vlanid:50/adsl/smart
```


Copyright © Huawei Technologies Co., Ltd.

5. Set the maximum number of MAC addresses that can be learned by the service port is 16. This parameter is to limit the maximum number of the MAC addresses that can be learned by one account, namely the maximum number of the PCs that can access the Internet through one account.

```
huawei(config)#mac-address max-mac-count service-port 1 16
```

Step 4 In the case of the SHDSL access mode, follow this procedure.

1. Configure an SHDSL profile. For details, see **Configuring SHDSL Profiles**. The ID of the SHDSL line profile is 3, the line rate is 2048 kbit/s, and the profile is used to activate 4-wire ports.

```
huawei(config)#shdsl line-profile quickadd 3 line four-wire rate 2048
```

2. Activate the SHDSL port. The port is port 0/3/1, and SHDSL line profile 3 and the default alarm profile (alarm profile 1) are bound to the port.

   NOTE

   By default, an ADSL port is in the activated state. Before binding a template to the port, you must deactivate the port.

```
huawei(config)#interface shl 0/3
huawei(config-if-shl-0/3)#deactivate 1
huawei(config-if-shl-0/3)#activate 1 3
huawei(config-if-shl-0/3)#alarm-config 1 1
huawei(config-if-shl-0/3)#quit
```

3. Run the **display traffic table ip** command to query the traffic profiles that exist in the system.

```
huawei(config)#display traffic table ip from-index 0
{ <cr>|to-index<K> }:

  Command:
          display traffic table ip from-index 0
  ------------------------------------------------------------------------------
   TID CIR      CBS      PIR      PBS      Pri Copy-policy         Pri-Policy
       (kbps)   (bytes)  (kbps)   (bytes)
  ------------------------------------------------------------------------------
     0 1024     34768    2048     69536      6 -                     tag-pri
     1 2496     81872    4992     163744     6 -                     tag-pri
     2 512      18384    1024     36768      0 -                     tag-pri
     3 576      20432    1152     40864      2 -                     tag-pri
     4 64       4048     128      8096       4 -                     tag-pri
     5 2048     67536    4096     135072     0 -                     tag-pri
     6 off      off      off      off        0 -                     tag-pri
  ------------------------------------------------------------------------------
  Total Num : 7
```

   According to service requirement, the user access rate is 2048 kbit/s. The query result shows that traffic profile 5 meets the requirement.

   NOTE

   - If no traffic profile in the system meets the service requirement, run the **traffic table ip** command to configure a new traffic profile.
   - On the MA5600T/MA5603T/MA5608T, the user access rate can be limited by either a traffic profile or an SHDSL line profile. When both profiles are configured, the user bandwidth adopts the minimum value in the two profiles. In this example, the traffic profile is used to limit the user access rate.

4. Run the **service-port** command to create a service port. The index of the new service virtual port is 2, the access port is port 0/3/1, traffic profile 5 meets the service requirement, and the S-VLAN is VLAN 50. The VPI and VCI must be the same as the management VPI and VCI of the peer modem. Assume that the management VPI and VCI of the modem are 1 and 39. To facilitate the maintenance of the service port, also configure the service port description.

Copyright © Huawei Technologies Co., Ltd.

```
huawei(config)#service-port 2 vlan 50 shdsl mode atm 0/3/1 vpi 1 vci 39 inbound
traffic-table
 index 5 outbound traffic-table index 5
huawei(config)#service-port desc 2 description MA5600T/MA5603T/MA5608THW/
Vlanid:50/shdsl/smart
```

5. Set the maximum number of MAC addresses that can be learned by the service port is 16. This parameter is to limit the maximum number of the MAC addresses that can be learned by one account, namely the maximum number of the PCs that can access the Internet through one account.

```
huawei(config)#mac-address max-mac-count service-port 2 16
```

Step 5 In the case of the VDSL access mode, follow this procedure.

In this example, the VDSL normal mode is used as an example.

1. Configure a VDSL profile. For details, see **Configuring VDSL2 Templates and Profiles**. Assume that the VDSL profile ID is 3, downstream rate is 2048 kbit/s, channel mode is the interleave mode, maximum downstream interleave delay is 8 ms, maximum upstream interleave delay is 2 ms, SNR margin is 6 dB, minimum downstream INP is 4, and minimum upstream INP is 2.

```
huawei(config)#vdsl line-profile quickadd 3 snr 60 0 300 60 0 300
huawei(config)#vdsl channel-profile quickadd 3 path-mode atm interleaved-delay
8 2 inp 4 2 rate
128 10000 128 10000 2048 2048
huawei(config)#vdsl line-template quickadd 3 line 3 channel1 3 100 100
```

2. Activate the VDSL port. The access port is port 0/4/1, and VDSL line template 3 and the default VDSL alarm template (alarm template 1) are bound to the port.

NOTE

By default, an ADSL port is in the activated state. Before binding a template to the port, you must deactivate the port.

```
huawei(config)#interface vdsl 0/4
huawei(config-if-vdsl-0/4)#deactivate 1
huawei(config-if-vdsl-0/4)#activate 1 template-index 3
huawei(config-if-vdsl-0/4)#alarm-config 1 1
huawei(config-if-vdsl-0/4)#quit
```

3. Run the **display traffic table ip** command to query the traffic profiles that exist in the system.

```
huawei(config)#display traffic table ip from-index 0
{ <cr>|to-index<K> }:

  Command:
          display traffic table ip from-index 0
  ------------------------------------------------------------------------------
   TID CIR      CBS      PIR      PBS      Pri Copy-policy         Pri-Policy
       (kbps)   (bytes)  (kbps)   (bytes)
  ------------------------------------------------------------------------------
     0 1024     34768    2048     69536      6 -                     tag-pri
     1 2496     81872    4992     163744     6 -                     tag-pri
     2 512      18384    1024     36768      0 -                     tag-pri
     3 576      20432    1152     40864      2 -                     tag-pri
     4 64       4048     128      8096       4 -                     tag-pri
     5 2048     67536    4096     135072     0 -                     tag-pri
     6 off      off      off      off        0 -                     tag-pri
  ------------------------------------------------------------------------------
  Total Num : 7
```

According to service requirement, the user access rate is 2048 kbit/s. The query result shows that traffic profile 5 meets the requirement.

Copyright © Huawei Technologies Co., Ltd.

NOTE

- If no traffic profile in the system meets the service requirement, run the **traffic table ip** command to configure a new traffic profile.
- On the MA5600T/MA5603T/MA5608T, the user access rate can be limited by either a traffic profile or a VDSL line profile. When both profiles are configured, the user bandwidth adopts the minimum value in the two profiles. In this example, the traffic profile is used to limit the user access rate.

4. Run the **service-port** command to create a service port. The index of the new service virtual port is 3, the access port is port 0/4/1, traffic profile 5 meets the service requirement, and the S-VLAN is VLAN 50. The VPI and VCI must be the same as the management VPI and VCI of the peer modem. Assume that the management VPI and VCI of the modem are 1 and 39. To facilitate the maintenance of the service port, also configure the service port description.

```
huawei(config)#service-port 3 vlan 50 vdsl mode atm 0/4/1 vpi 1 vci 39 inbound
traffic-table index 5 outbound
 traffic-table index 5
huawei(config)#service-port desc 3 description MA5600T/MA5603T/MA5608THW/
Vlanid:50/vdsl/smart
```

5. Set the maximum number of MAC addresses that can be learned by the service port is 16. This parameter is to limit the maximum number of the MAC addresses that can be learned by one account, namely the maximum number of the PCs that can access the Internet through one account.

```
huawei(config)#mac-address max-mac-count service-port 3 16
```

Step 6 Enable the IPoA-IPoE protocol conversion.

This step is to configure the IPoA MAC address pool. The start MAC address in the MAC address pool is 0000-1111-1010, and the maximum number of the MAC addresses in the MAC address pool is 300. The IPoA-IPoE protocol conversion is enabled, the default gateway is the same as the IP address (192.168.1.20) of the upper-layer router, and the service encapsulation mode is LLC-IPoA. The IP address of the modem is 192.168.1.1.

```
huawei(config)#mac-pool xpoa 0000-1111-1010 300
huawei(config)#ipoa enable
huawei(config)#ipoa default gateway 192.168.1.20
huawei(config)#encapsulation 0/2/0 vpi 1 vci 39 type ipoa llc srcIP 192.168.1.1
huawei(config)#encapsulation 0/3/1 vpi 1 vci 39 type ipoa llc srcIP 192.168.1.1
huawei(config)#encapsulation 0/4/1 vpi 1 vci 39 type ipoa llc srcIP 192.168.1.1
```

Step 7 Save the data.

```
huawei(config)#save
```

----End

Verification

- Step 1: Set the VPI/VCI of the modem to 1/39, encapsulation mode to llc-ipoa, and IP address to 192.168.1.1.
- Step 2: After the settings on the modem are completed, the network connection is automatically set up and the user can access the Internet.
- Step 3: When downloading files through FTP, you can open **Task Manager** in Windows and click **Networking** to check the link rate. Calculate the Internet access rate by the formula: Attainable Internet access rate = Computer NIC rate/48 x 53 x 8. The calculated result approximates to the planned 2048 kbit/s.

Copyright © Huawei Technologies Co., Ltd.

Configuration File

Configuration File of the ADSL access mode:

```
vlan 50 smart
port vlan 50 0/19 0
port vlan 50 0/19 1
link-aggregation 0/19 0 0/19 1 egress-ingress workmode lacp-static
adsl line-profile quickadd 3 2 snr 60 30 120 60 30 120
adsl channel-profile quickadd 3 interleaved-delay 10 10 rate 1024 2048 3096 1024
2048 3096
adsl line-template quickadd 3 line 3 channel1 3 60 70 channel2 3
interface adsl 0/2
deactivate 0
activate 0 template-index 3
alarm-config 0 1
quit
service-port 1 vlan 50 adsl 0/2/0 vpi 1 vci 39 inbound traffic-table index 5
outbound traffic-table index 5
service-port desc 1 description MA5600T/MA5603T/MA5608THW/Vlanid:50/adsl/smart
mac-address max-mac-count service-port 1 16
mac-pool xpoa 0000-1111-1010 300
ipoa enable
ipoa default gateway 192.168.1.20
encapsulation 0/2/0 vpi 1 vci 39 type ipoa llc srcIP 192.168.1.1
save
```

Configuration File of the SHDSL access mode:

```
vlan 50 smart
port vlan 50 0/19 0
port vlan 50 0/19 1
link-aggregation 0/19 0 0/19 1 egress-ingress workmode lacp-static
shdsl line-profile quickadd 3 line four-wire rate 2048
interface shl 0/3
deactivate 1
activate 1 3
alarm-config 1 1
quit
service-port 2 vlan 50 shdsl mode atm 0/3/1 vpi 1 vci 39 inbound traffic-table index
5 outbound traffic-table index 5
service-port desc 2 description MA5600T/MA5603T/MA5608THW/Vlanid:50/shdsl/smart
mac-address max-mac-count service-port 2 16
mac-pool xpoa 0000-1111-1010 300
ipoa enable
ipoa default gateway 192.168.1.20
encapsulation 0/3/1 vpi 1 vci 39 type ipoa llc srcIP 192.168.1.1
save
```

Configuration File of the VDSL access mode:

```
vlan 50 smart
port vlan 50 0/19 0
port vlan 50 0/19 1
link-aggregation 0/19 0 0/19 1 egress-ingress workmode lacp-static
vdsl line-profile quickadd 3 snr 60 0 300 60 0 300
vdsl channel-profile quickadd 3 path-mode atm interleaved-delay 8 2 inp 4 2 rate
128 10000 128 10000 2048 2048
interface vdsl 0/4
deactivate 1
activate 1 template-index 3
alarm-config 1 1
quit
service-port 3 vlan 50 vdsl mode atm 0/4/1 vpi 1 vci 39  inbound traffic-table index
5 outbound traffic-table index 5
service-port desc 3 description MA5600T/MA5603T/MA5608THW/Vlanid:50/vdsl/smart
mac-address max-mac-count service-port 3 16
```


Copyright © Huawei Technologies Co., Ltd.

```
mac-pool xpoa 0000-1111-1010 300
ipoa enable
ipoa default gateway 192.168.1.20
encapsulation 0/4/1 vpi 1 vci 39 type ipoa llc srcIP 192.168.1.1
save
```

3.1.5 Example: Configuring the Internet Access Service in the xDSL 802.1X Mode

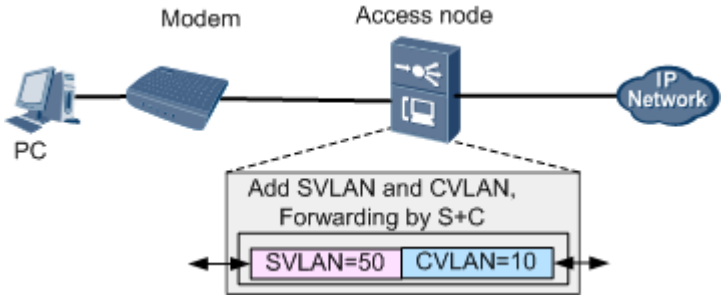
This topic describes how to configure a user to access the MA5600T/MA5603T/MA5608T in the xDSL mode, and then access the Internet in the 802.1X authentication mode at a rate of 2048 kbit/s.

Service Requirements

- The user accesses the Internet in the 802.1X authentication mode and is authenticated locally.
- User packets are tagged with two VLAN tags and then transmitted upstream. The outer VLAN tag is used to identify the service. The inner VLAN tag is used to identify the user. The service of each user is identified by S+C, which is a 1:1 access scenario.
- The user access rate is 2048 kbit/s, which is restricted by the traffic profile.
- Dual GE ports are adopted for upstream transmission to ensure reliability. Link aggregation is configured for the two upstream ports.

Figure 3-5 shows an example network of the Internet access service in the xDSL 802.1X mode.

Figure 3-5 Example network of the Internet access service in the xDSL IPoE mode



Prerequisite

- The user already installs the client software that supports 802.1X.
- The user name and the password for authentication are already configured properly on the RADIUS server.

Procedure

Step 1 Configure a VLAN.

Configure S-VLAN 50 with the stacking attribute. The user packet goes upstream carrying two VLAN tags. The outer VLAN tag identifies the service and the inner VLAN tag identifies the

Copyright © Huawei Technologies Co., Ltd.

user. The service of each user is identified by unique S-VLAN+C-VLAN, and the VLAN forwarding mode is the S-VLAN+C-VLAN mode.

```
huawei(config)#vlan 50 smart
huawei(config)#vlan attrib 50 stacking
huawei(config)#vlan forwarding 50 vlan-connect
```

Step 2 Configure upstream ports.

Add upstream ports 0/19/0 and 0/19/1 to VLAN 50. Two ports are added for the purpose of port aggregation.

```
huawei(config)#port vlan 50 0/19 0
huawei(config)#port vlan 50 0/19 1
```

To aggregate the two upstream ports as one aggregation group, set the packet forwarding mode of the aggregation group to egress-ingress, and set the aggregation group to work in the LACP static mode, do as follows:

```
huawei(config)#link-aggregation 0/19 0 0/19 1 egress-ingress workmode lacp-static
```

NOTE

The aggregated ports must meet the following requirements: The ports must work in the full-duplex mode; the port rates must be the same and the rate of an electrical port must not be of the auto-negotiation type; the attributes of the ports, such as the default VLAN ID (PVID) and VLAN, must be the same; one port can belong to only one aggregation group; the port must not be a mirroring destination port; the port must not be in the auto-negotiation mode; the start port ID must be smaller than the end port ID.

Step 3 In the ADSL access mode, follow this procedure.

1. Configure an ADSL2+ profile. For details, see Configuring ADSL2+ Profiles. The default ADSL2+ line template (line template 1) and the default ADSL2+ alarm template (alarm template 1) are used as an example.
2. Activate the ADSL port, and bind the ADSL2+ templates.

   NOTE

   By default, an ADSL port is in the activated state. Before binding a template to the port, you must deactivate the port.

   In the ADSL access mode, bind the default ADSL2+ line template 1 and ADSL2+ alarm template 1 to ADSL port 0/2/0.

   ```
   huawei(config)#interface adsl 0/2
   huawei(config-if-adsl-0/2)#deactivate 0
   huawei(config-if-adsl-0/2)#activate 0 profile-index 1
   huawei(config-if-adsl-0/2)#alarm-config 0 1
   huawei(config-if-adsl-0/2)#quit
   ```

3. Run the **display traffic table** command to query the existing traffic profiles in the system.

   ```
   huawei(config)#display traffic table ip from-index 0
   { <cr>|to-index<K> }:

     Command:
             display traffic table ip from-index 0
     ------------------------------------------------------------------------------
      TID CIR      CBS      PIR      PBS      Pri Copy-policy         Pri-Policy
          (kbps)   (bytes)  (kbps)   (bytes)
     ------------------------------------------------------------------------------
        0 1024     34768    2048     69536      6 -                     tag-pri
        1 2496     81872    4992     163744     6 -                     tag-pri
        2 512      18384    1024     36768      0 -                     tag-pri
        3 576      20432    1152     40864      2 -                     tag-pri
        4 64       4048     128      8096       4 -                     tag-pri
        5 2048     67536    4096     135072     0 -                     tag-pri
        6 off      off      off      off        0 -                     tag-pri
   ```


Copyright © Huawei Technologies Co., Ltd.

```
------------------------------------------------------------------------------
Total Num : 7
```

According to service requirements, the user access rate is 2048 kbit/s. The query result shows that traffic profile 5 (for inbound and outbound rate limitation) meets the requirements.

NOTE

- If a matched traffic profile is not available in the system, run the **traffic table ip** command to configure a new traffic profile.
- On the MA5600T/MA5603T/MA5608T, the user access rate can be limited by either a traffic profile or an ADSL line profile. When both profiles are configured, the smaller one of the two rates configured in the profiles is adopted as the user bandwidth. In this example, the traffic profile is used to limit the user access rate.

4. Run the **service-port** command to create a service port, adopt traffic profile 5, and set the S-VLAN ID to 50. The index of the service port is 1, and the VPI and VCI of the service port must be the same as the management VPI and VCI of the peer modem. Assume that the management VPI and VCI of the modem are 1 and 39, and the access port ID is 0/2/0. To facilitate the maintenance of the service port, also configure the service port description.

```
huawei(config)#service-port 1 vlan 50 adsl 0/2/0 vpi 1 vci 39 inbound traffic-table index 5 outbound traffic-table index 5
huawei(config)#service-port desc 1 description Vlanid:50/adsl/vpi:1vci:39/stacking
```

5. Set the C-VLAN ID of the preset service port 1 to 10 for identifying the user. Configure the important user packet with a higher priority so that the user packet can be processed with precedence, and set the priority of the inner VLAN to 4.

```
huawei(config)#stacking label service-port 1 10
huawei(config)#stacking inner-priority service-port 1 4
```

Step 4 In the SHDSL access mode, follow this procedure.

1. Configure an SHDSL profile. For details, see Configuring SHDSL Profiles. Add SHDSL line profile 3 of the PTM type, with the maximum line rate 2048 kbit/s.

```
huawei(config)#shdsl line-profile quickadd 3 ptm rate 512 2048
```

2. Activate SHDSL port 0/3/1, and bind the preset SHDSL line profile 3 and the default SHDSL alarm template (alarm template 1) to the port.

NOTE

By default, an SHDSL port is in the activated state. Before binding a profile or template to the port, you must deactivate the port.

```
huawei(config)#interface shl 0/3
huawei(config-if-shl-0/3)#deactivate 1
huawei(config-if-shl-0/3)#activate 1 3
huawei(config-if-shl-0/3)#alarm-config 1 1
huawei(config-if-shl-0/3)#quit
```

3. Run the **display traffic table** command to query the existing traffic profiles in the system.

```
huawei(config)#display traffic table ip from-index 0
{ <cr>|to-index<K> }:

  Command:
          display traffic table ip from-index 0
  ------------------------------------------------------------------------------
   TID CIR      CBS      PIR      PBS      Pri Copy-policy         Pri-Policy
       (kbps)   (bytes)  (kbps)   (bytes)
  ------------------------------------------------------------------------------
     0 1024     34768    2048     69536      6 -                     tag-pri
```


Copyright © Huawei Technologies Co., Ltd.

```
  1 2496     81872    4992     163744     6 -                        tag-pri
  2 512      18384    1024     36768      0 -                        tag-pri
  3 576      20432    1152     40864      2 -                        tag-pri
  4 64       4048     128      8096       4 -                        tag-pri
  5 2048     67536    4096     135072     0 -                        tag-pri
  6 off      off      off      off        0 -                        tag-pri
-------------------------------------------------------------------------------
Total Num : 7
```

According to service requirements, the user access rate is 2048 kbit/s. The query result shows that traffic profile 5 (for inbound and outbound rate limitation) meets the requirements.

NOTE

- If a matched traffic profile is not available in the system, run the **traffic table ip** command to configure a new traffic profile.
- On the MA5600T/MA5603T/MA5608T, the user access rate can be limited by either a traffic profile or an SHDSL line profile. When both profiles are configured, the smaller one of the two rates configured in the profiles is adopted as the user bandwidth. In this example, the traffic profile is used to limit the user access rate.

4. Run the **service-port** command to create a service port, adopt traffic profile 5, and set the S-VLAN ID to 50. Set the SHDSL channel mode to PTM, and create service port 2 on SHDSL port 0/3/1. To facilitate the maintenance of the service port, also configure the service port description.

```
huawei(config)#service-port 2 vlan 50 shdsl mode ptm 0/3/1 inbound traffic-
table
 index 5 outbound traffic-table index 5
huawei(config)#service-port desc 2 description Vlanid:50/shdsl/vpi:1vci:39/
stacking
```

5. Set the C-VLAN ID of the preset service port 2 to 10 for identifying the user. Configure the important user packet with a higher priority so that the user packet can be processed with precedence, and set the priority of the inner VLAN to 4.

```
huawei(config)#stacking label service-port 2 10
huawei(config)#stacking inner-priority service-port 2 4
```

Step 5 In the VDSL access mode, follow this procedure.

In this example, the VDSL normal mode is used as an example.

1. Configure a VDSL profile. For details, see Configuring VDSL2 Templates and Profiles. Assume that the VDSL profile ID is 3, downstream rate is 2048 kbit/s, channel mode is the interleave mode, maximum downstream interleave delay is 8 ms, maximum upstream interleave delay is 2 ms, SNR margin is 6 dB, minimum downstream INP is 4, and minimum upstream INP is 2.

```
huawei(config)#vdsl line-profile quickadd 3 snr 60 0 300 60 0 300
huawei(config)#vdsl channel-profile quickadd 3 path-mode ptm interleaved-delay
8 2 inp 4 2 rate
128 10000 128 10000 2048 2048
huawei(config)#vdsl line-template quickadd 3 line 3 channel1 3 100 100
```

2. Activate VDSL port 0/4/1, and bind the preset VDSL line template 3 and the default VDSL alarm template (alarm template 1) to the port.

NOTE

By default, a VDSL port is in the activated state. Before binding a template to the port, you must deactivate the port.

```
huawei(config)#interface vdsl 0/4
huawei(config-if-vdsl-0/4)#deactivate 1
```


Copyright © Huawei Technologies Co., Ltd.

```
huawei(config-if-vdsl-0/4)#activate 1 template-index 3
huawei(config-if-vdsl-0/4)#alarm-config 1 1
huawei(config-if-vdsl-0/4)#quit
```

3. Run the **display traffic table** command to query the existing traffic profiles in the system.

```
huawei(config)#display traffic table ip from-index 0
{ <cr>|to-index<K> }:

  Command:
          display traffic table ip from-index 0
  ------------------------------------------------------------------------------
   TID CIR      CBS      PIR      PBS      Pri Copy-policy         Pri-Policy
       (kbps)   (bytes)  (kbps)   (bytes)
  ------------------------------------------------------------------------------
     0 1024     34768    2048     69536      6 -                     tag-pri
     1 2496     81872    4992     163744     6 -                     tag-pri
     2 512      18384    1024     36768      0 -                     tag-pri
     3 576      20432    1152     40864      2 -                     tag-pri
     4 64       4048     128      8096       4 -                     tag-pri
     5 2048     67536    4096     135072     0 -                     tag-pri
     6 off      off      off      off        0 -                     tag-pri
  ------------------------------------------------------------------------------
  Total Num : 7
```

According to service requirements, the user access rate is 2048 kbit/s. The query result shows that traffic profile 5 (for inbound and outbound rate limitation) meets the requirements.

NOTE

- If a matched traffic profile is not available in the system, run the **traffic table ip** command to configure a new traffic profile.
- On the MA5600T/MA5603T/MA5608T, the user access rate can be limited by either a traffic profile or a VDSL line profile. When both profiles are configured, the smaller one of the two rates configured in the profiles is adopted as the user bandwidth. In this example, the traffic profile is used to limit the user access rate.

4. Run the **service-port** command to create a service port, adopt traffic profile 5, and set the S-VLAN ID to 50. Set the VDSL channel mode to PTM, and create service port 3 on VDSL port 0/4/1. To facilitate the maintenance of the service port, also configure the service port description.

```
huawei(config)#service-port 3 vlan 50 vdsl mode ptm 0/4/1 inbound traffic-
table
index 5 outbound traffic-table index 5
huawei(config)#service-port desc 3 description Vlanid:50/vdsl/vpi:1vci:39/
stacking
```

5. Set the C-VLAN ID of the preset service port 3 to 10 for identifying the user. Configure the important user packet with a higher priority so that the user packet can be processed with precedence, and set the priority of the inner VLAN to 4.

```
huawei(config)#stacking label service-port 3 10
huawei(config)#stacking inner-priority service-port 3 4
```

Step 6 Configure the 802.1X authentication.

1. Enable the 802.1X global switch. Enable the 802.1X authentication for ports 1, 2, and 3. The 802.1X needs to be triggered by DHCP. Therefore, the DHCP-trigger authentication must be enabled.

```
huawei(config)#dot1x enable
huawei(config)#dot1x service-port 1
huawei(config)#dot1x service-port 2
huawei(config)#dot1x service-port 3
huawei(config)#dot1x dhcp-trigger enable
```


Copyright © Huawei Technologies Co., Ltd.

2. Configure an 802.1X parameters. In the local termination authentication, the 802.1X parameters should be configured to be in the EAP termination mode. The count of allowed handshake failure is 1 and the handshake interval is 20s.

```
huawei(config)#dot1x keepalive retransmit 1 interval 20 service-port 1
huawei(config)#dot1x keepalive retransmit 1 interval 20 service-port 2
huawei(config)#dot1x keepalive retransmit 1 interval 20 service-port 3
huawei(config)#dot1x eap-end service-port 1
huawei(config)#dot1x eap-end service-port 2
huawei(config)#dot1x eap-end service-port 3
```

3. Name the AAA authentication scheme **huawei** and name the AAA accounting scheme **huawei**. During the local authentication, the AAA authentication scheme is a local authentication. Therefore, you do not need to configure the RADIUS server profile; however, you need to configure the accounting mode in the accounting scheme to **none**.

```
huawei(config)#aaa
huawei(config-aaa)#authentication-scheme huawei
huawei(config-aaa-authen-huawei)#authentication-mode local
huawei(config-aaa-authen-huawei)#quit
huawei(config-aaa)#accounting-scheme huawei
huawei(config-aaa-accounting-huawei)#accounting-mode none
huawei(config-aaa-accounting-huawei)#quit
```

4. Create a local user with the user name **shenzhen** and the password **shenzhen**.

```
huawei(config-aaa)#local-user shenzhen@huawei service-type terminal password
shenzhen
```

5. Name the AAA domain **huawei**. Bind the domain with the accounting scheme named **huawei**, authentication scheme named **huawei**.

```
huawei(config-aaa)#domain huawei
huawei(config-aaa-domain-huawei)#authentication-scheme huawei
huawei(config-aaa-domain-huawei)#accounting-scheme huawei
huawei(config-aaa-domain-huawei)#quit
huawei(config-aaa)#quit
```

Step 7 Save the data.

```
huawei(config)#save
```

----End

Verification

The procedure for triggering the 802.1X client by DHCP in the Windows XP OS is as follows:

- Step 1: Choose **Start** > **Control Panel** > **Network Connections**. Right-click **Local Area Connection** and then choose **Properties**.
- Step 2: In the dialog box that is displayed,
  1. On the **General** tab page, set **Internet Protocol (TCP/IP)** to **Obtain an IP address automatically**.
  2. On the **Authentication** tab page, select **Enable IEEE 802.1x authentication for this network**.
  3. Click **OK**.
- Step 3: Right-click **Local Area Connection** and then choose **Disable**.
- Step 4: Right-click **Local Area Connection** and then choose **Enable**.
- After a while, the **modem2** prompt icon will be displayed in the lower right corner on the PC desktop. Click the icon. In the dialog box that is displayed, enter the user name

Copyright © Huawei Technologies Co., Ltd.

shenzhen and the password **shenzhen**, and then click **OK** to start the actual service authentication. After passing the authentication, you can access the Internet.

- When a file is downloaded through FTP, you can open Windows Task Manager and then click **Networking** to observe the link speed. Calculate the Internet access rate by the formula: Attainable Internet access rate = Computer network adapter rate/48 x 53 x 8. The calculated result approximates to the planned 2048 kbit/s.

Configuration File

Configuration File of the ADSL access mode:

```
vlan 50 smart
vlan attrib 50 stacking
vlan forwarding 50 vlan-connect
port vlan 50 0/19 0
port vlan 50 0/19 1
link-aggregation 0/19 0 0/19 1 egress-ingress workmode lacp-static
interface adsl 0/2
deactivate 0
activate 0 template-index 1
alarm-config 0 1
quit
service-port 1 vlan 50 adsl 0/2/0 vpi 1 vci 39 inbound traffic-table index 5
outbound traffic-table index 5
service-port desc 1 description Vlanid:50/adsl/vpi:1vci:39/stacking
stacking label service-port 1 10
stacking inner-priority service-port 1 4
dot1x enable
dot1x service-port 1
dot1x dhcp-trigger enable
dot1x keepalive retransmit 1 interval 20 service-port 1
dot1x eap-end service-port 1
aaa
authentication-scheme huawei
authentication-mode local
quit
accounting-scheme huawei
accounting-mode none
quit
local-user shenzhen@huawei service-type terminal password shenzhen
domain huawei
authentication-scheme huawei
accounting-scheme huawei
quit
quit
save
```

Configuration File of the SHDSL access mode:

```
vlan 50 smart
vlan attrib 50 stacking
vlan forwarding 50 vlan-connect
port vlan 50 0/19 0
port vlan 50 0/19 1
link-aggregation 0/19 0 0/19 1 egress-ingress workmode lacp-static
shdsl line-profile quickadd 3 ptm rate 512 2048
interface shl 0/3
deactivate 1
activate 1 3
alarm-config 1 1
quit
service-port 2 vlan 50 shdsl mode ptm 0/3/1 inbound traffic-table index 5 outbound
traffic-table index 5
service-port desc 2 description Vlanid:50/shdsl/vpi:1vci:39/stacking
```


Copyright © Huawei Technologies Co., Ltd.

```
stacking label service-port 2 10
stacking inner-priority service-port 2 4
dot1x enable
dot1x service-port 2
dot1x dhcp-trigger enable
dot1x keepalive retransmit 1 interval 20 service-port 2
dot1x eap-end service-port 2
aaa
authentication-scheme huawei
authentication-mode local
quit
accounting-scheme huawei
accounting-mode none
quit
local-user shenzhen@huawei service-type terminal password shenzhen
domain huawei
authentication-scheme huawei
accounting-scheme huawei
quit
quit
save
```

Configuration File of the VDSL access mode:

```
vlan 50 smart
vlan attrib 50 stacking
vlan forwarding 50 vlan-connect
port vlan 50 0/19 0
port vlan 50 0/19 1
link-aggregation 0/19 0 0/19 1 egress-ingress workmode lacp-static
vdsl line-profile quickadd 3 snr 60 0 300 60 0 300
vdsl channel-profile quickadd 3 path-mode ptm interleaved-delay 8 2 inp 4 2 rate
128 10000 128 10000 2048 2048
interface vdsl 0/4
deactivate 0
activate 0 template-index 3
alarm-config 0 1
quit
service-port 3 vlan 50 vdsl mode ptm 0/4/1 inbound traffic-table index 5 outbound
traffic-table index 5
service-port desc 3 description Vlanid:50/vdsl/vpi:1vci:39/stacking
stacking label service-port 3 10
stacking inner-priority service-port 3 4
stacking inner-priority service-port 2 4
dot1x enable
dot1x service-port 3
dot1x dhcp-trigger enable
dot1x keepalive retransmit 1 interval 20 service-port 3
dot1x eap-end service-port 3
aaa
authentication-scheme huawei
authentication-mode local
quit
accounting-scheme huawei
accounting-mode none
quit
local-user shenzhen@huawei service-type terminal password shenzhen
domain huawei
authentication-scheme huawei
accounting-scheme huawei
quit
quit
save
```


Copyright © Huawei Technologies Co., Ltd.

3.1.6 Configuration Example of Changing ADSL Internet Access Service to VDSL Internet Access Service (for the VDSL2 Board)

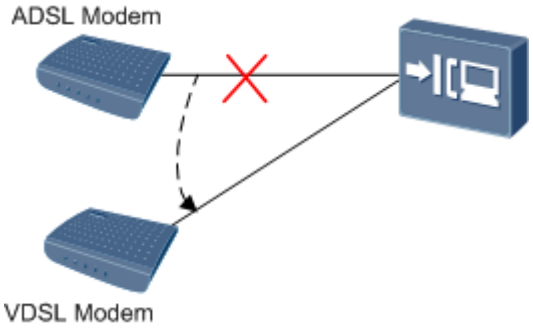
Driven by customer demands for higher bandwidth, the ADSL Internet access service of the VDSL2 board needs to change to the VDSL2 Internet access service. This topic describes how to achieve so.

Service Requirements

- During network restructuring, the ADSL Internet access service of the VDSL2 board needs to change to the VDSL2 Internet access service.
- Users request a higher bandwidth of 8192 kbit/s.
- The VDSL modem is a PTM-mode modem that uses the G993.2 profile 12a.
- Users expect that new requirements are met by modifying certain configurations of the original ADSL service alone. PITP (protecting user accounts from theft), roaming, and upstream link aggregation are configured.

Figure 3-6 shows an example network of the Internet access service through PPPoE dialup.

Figure 3-6 Example network of the Internet access service through PPPoE dialup



Prerequisite

- The AAA function must be configured.
  - To enable the AAA function on the device, see **2.4 Configuring AAA**.
  - If the AAA function is implemented by the BRAS, a connection to the BRAS must be established. The BRAS should be capable of identifying the VLAN tag of the MA5600T/MA5603T/MA5608T in the upstream direction. For the identification purpose, the user name and password for dial-up Internet access must be configured on the BRAS.

Procedure

Step 1 Confirm the line template bound to a port that needs such service modifications, for example, port 0/2/4.

Run the **display port state** command to query the line template bound to the port.

Copyright © Huawei Technologies Co., Ltd.

```
huawei(config)#interface vdsl 0/2
huawei(config-if-vdsl-0/2)#display port state 4
  ------------------------------------------------------------------------------
  Port     Status          Loopback   Line Template Alarm Template Bonding-group
  ------------------------------------------------------------------------------
   4     Activated          Disable             10              1             -
  ------------------------------------------------------------------------------
```

The query result shows that line template 10 is bound to port 4. Run the **display vdsl line-template** command to query the channel profile and line profile in the line template.

```
huawei(config-if-vdsl-0/2)#display vdsl line-template 10
  ------------------------------------------------------------------------------
  Template index: 10     Name: VDSL LINE TEMPLATE 10
  Line profile index                          : 1
  Channel1 profile index                      : 10
  Channel1 rate adaptation ratio downstream   : 100
  Channel1 rate adaptation ratio upstream     : 100
  ------------------------------------------------------------------------------
```

Step 2 Confirm whether to change the transmission mode and signal noise ratio (SNR).

The query result shows that line profile 1 and channel profile 10 are in line template 10. Run the **display vdsl line-profile** command to query the transmission mode and SNR configured in the line profile.

```
huawei(config-if-vdsl-0/2)#display vdsl line-profile
1
  ------------------------------------------------------------------------------
  Profile index: 1      Name: DEFVAL
  Transmission mode:
    T1.413                          G.992.1(Annex A/B/C)
    G.992.2(Annex A/C)              G.992.3(Annex A/B/I/J/L/M)
    G.992.4(Annex A/I)              G.992.5(Annex A/B/I/J/M)
    G.993.2(Annex A/B/C)
  Bit swap downstream                             : Enable
  Bit swap upstream                               : Enable
  Form of transmit rate adaptation downstream     : AdaptAtStartup
  Form of transmit rate adaptation upstream       : AdaptAtStartup
  Target SNR margin downstream(0.1dB)             : 60
  Minimum SNR margin downstream(0.1dB)            : 0
  Maximum SNR margin downstream(0.1dB)            : 300
  Target SNR margin upstream(0.1dB)               : 60
  Minimum SNR margin upstream(0.1dB)              : 0
  Maximum SNR margin upstream(0.1dB)              : 300
  UPBO US1 band reference PSD parameters[a, b]    : 1650,1020
  UPBO US2 band reference PSD parameters[a, b]    : 1650,615
  UPBO US3 band reference PSD parameters[a, b]    : 0,0
  UPBO US4 band reference PSD parameters[a, b]    : 0,0
---- More ( Press 'Q' to break ) ----
```

- If the transmission mode is ADSL, change the transmission mode to VDSL or ALL. To do so, proceed to **Step 3**.
- If the SNR value does not meet actual requirements over the live network, change it according to actual conditions. To do so, proceed to **Step 3**.
- If the transmission mode is VDSL or ALL and the SNR value also meets actual conditions over the live network, go to **Step 4**.

Step 3 Run the **vdsl line-profile quickadd** command to reconfigure the transmission mode and SNR. In addition, configure exclusive VDSL parameters.

1. According to actual conditions over the live network, SNR is planned to 7 dB, transmission mode to all (its value is 1), and line profile index to 11.

Copyright © Huawei Technologies Co., Ltd.

```
huawei(config-if-vdsl-0/2)#vdsl line-profile quickadd 11 transmode 1 snr 70 0
300 70 0 300
```

2. All parameters following **vdsl-parameter** are VDSL parameters in contrast to ADSL. These parameters do not need to be configured in the case of the ADSL Internet access service. However, in the case of the VDSL Internet access service, these parameters need to be configured according to actual conditions. The default G993.2 profile is profile 12a, which is consistent with the required profile in this example. Hence, no modification is required.

Step 4 Run the **display vdsl channel-profile** command to query the data path mode and line rate in the channel profile.

```
huawei(config-if-vdsl-0/2)#display vdsl channel-profile
10
  ---------------------------------------------------------------------------
  Profile index: 10      Name: VDSL CHANNEL PROFILE 10
  Data path mode                                  : ATM
  Minimum impulse noise protection downstream     : NoProtection
  Minimum impulse noise protection upstream       : NoProtection
  Maximum interleaving delay downstream(ms)       : 20
  Maximum interleaving delay upstream(ms)         : 20
  Minimum transmit rate downstream(Kbps)          : 32
  Minimum reserved transmit rate downstream(Kbps) : 32
  Maximum transmit rate downstream(Kbps)          : 200000
  Minimum transmit rate upstream(Kbps)            : 32
  Minimum reserved transmit rate upstream(Kbps)   : 32
  Maximum transmit rate upstream(Kbps)            : 200000
---- More ( Press 'Q' to break ) ----
```

If the line rate does not meet the requirements of users, change it. To do so, proceed to **Step 5**.

Step 5 Run the **vdsl channel-profile quickadd** command to reconfigure the data path mode and line rate.

To meet customer demands, increase bandwidth to 8192 kbit/s, set the data path mode to both and add a new channel profile (channel profile 11).

```
huawei(config-if-vdsl-0/2)#vdsl channel-profile quickadd 11 path-mode both rat
e 32 81920 32 2048
```

Step 6 Bind the required VDSL2 line template 11 to port 0/2/4.

NOTE

By default, a port is in the activated state. Before binding a template to the port, you must deactivate the port.

```
huawei(config-if-vdsl-0/2)#vdsl line-template quickadd 11 line 11 channel1 11 100
100
huawei(config-if-vdsl-0/2)#deactivate 4
huawei(config-if-vdsl-0/2)#activate 4 template-index 11
huawei(config-if-vdsl-0/2)#quit
```

Step 7 Add a traffic profile.

1. Run the **display traffic table ip** command to query the existing traffic profiles in the system.

```
huawei(config)#display traffic table ip from-index 0
{ <cr>|to-index<K> }:

  Command:
          display traffic table ip from-index 0
  ------------------------------------------------------------------------------
   TID CIR       CBS       PIR       PBS       Pri Copy-policy         Pri-Policy
       (kbps)    (bytes)   (kbps)    (bytes)
  ------------------------------------------------------------------------------
     0 1024      34768     2048      69536      6 -                     tag-pri
     1 2496      81872     4992      163744     6 -                     tag-pri
```


Copyright © Huawei Technologies Co., Ltd.

```
  2 512      18384    1024     36768      0 -                          tag-pri
  3 576      20432    1152     40864      2 -                          tag-pri
  4 64       4048     128      8096       4 -                          tag-pri
  5 2048     67536    4096     135072     0 -                          tag-pri
  6 off      off      off      off        0 -                          tag-pri
-------------------------------------------------------------------------------
Total Num : 7
```

According to customer requirements, the user access rate is 8192 kbit/s. The query result shows that no traffic profile meets customer requirements. Therefore, run the **traffic table ip** command to configure a new traffic profile (traffic profile 7) and set the rate to 8192 kbit/s in the new traffic profile.

NOTE

You can configure the traffic profile or the VDSL2 line profile on the MA5600T/MA5603T/MA5608T to limit the user access rate. When both profiles are configured, the bandwidth of the user is the minimum value of the two profiles. In this example, the traffic profile is used to limit the user access rate.

```
huawei(config)#traffic table ip index 7 cir 8192 priority 6 priority-policy
local-Setting
```

Step 8 Configure a service port.

Run the **display service-port** command to query the original service port.

```
huawei(config)#display service-port port 0/2/4
{ <cr>|autosense<K>|ont<K>|sort-by<K> }:

  Command:
          display service-port port 0/2/4
  Switch-Oriented Flow List
  -------------------------------------------------------------------------------
  INDEX VLAN VLAN     PORT F/ S/ P VPI  VCI   FLOW  FLOW       RX   TX   STATE
        ID   ATTR     TYPE                    TYPE  PARA
  -------------------------------------------------------------------------------
      5  101 common   vdl  0/2/4  0    35    vlan  untag      6    6    up
  -------------------------------------------------------------------------------
   Total : 1  (Up/Down :    1/0)
```

The query result shows that VPI and VCI are configured, which indicate that VDSL is in the ATM mode. In this example, however, the VDSL is in the PTM mode. Run the **service-port** command to create a service port, adopt traffic profile 7, and set the S-VLAN ID to 101. Set the index of the service port to 3 (the index must be different from the original index) and the access port to 0/2/4. To facilitate maintenance of the service port, configure the service port description.

NOTE

Generally, the ADSL is in the ATM mode and the VDSL is in the PTM mode. If an ATM service port only is configured, a PTM service port needs to be added.

```
huawei(config)#service-port 3 vlan 101 vdsl mode ptm 0/2/4 rx-cttr 7 tx-cttr 7
huawei(config)#service-port desc 3 description Vlanid:101/vdsl/ptm
```

Step 9 Save the data.

```
huawei(config)#save
```

----End

Verification

- Step 1: Configure the user name and password for the dialup on the modem (the user name and password must be the same as those configured on the BRAS).

Copyright © Huawei Technologies Co., Ltd.

- Step 2: Dial up on the PC by using the PPPoE dialup software. After the dialup is successful, the user can access the Internet.
- Step 3: When FTP is used to download files and after the dialup is performed on the PPPoE dialup software, the PPPoE dialup software prompts that the dialup is successful. Then, the PC can access the Internet in the PPPoE mode.
- Step 4: When downloading files through FTP, you can open Task Manager in Windows and click Networking to check the link speed. Then, you can calculate the Internet access rate by the following formula: Attainable Internet access rate = Computer network adapter rate/48 x 53 x 8. The calculated result approximates to the planned 8192 kbit/s.

3.2 Example: Configuring the xDSL Multicast Service

This topic describes how to configure the multicast video service.

3.2.1 Configuration Example of the Multicast Video Service (Static Program Configuration)

Static program configuration for multicast services is fine-grained program configuration and management, with functions of program/user multicast bandwidth management, program preview, and program prejoin. This configuration mode applies to multicast services that have strict requirements on program and user management.

Service Requirements

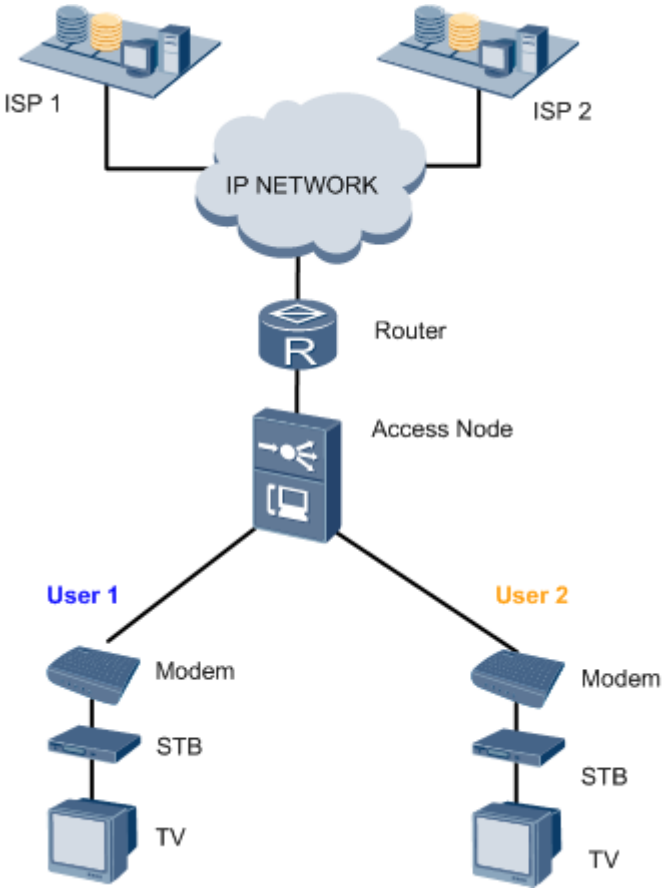
- ISP 1 has two popular music programs, and ISP 2 has one popular music program and one popular video program. These programs can be ordered continuously and in time.
- The program ordering status can be recorded, collected, and reported for monitoring and charging.
- User 1 has purchased only the music program package from ISP 1, while user 2 has purchased only the video program package from ISP 2. Rights management is required for the two users.
- The package purchased by user 1 limits the maximum available multicast bandwidth to 10 Mbit/s, and the package purchased by user 2 limits the maximum available multicast bandwidth to 5 Mbit/s. Bandwidth restriction is required for the two users.

Figure 3-7 shows an example network of the multicast service.

User 1 and user 2 are connected to the MA5600T/MA5603T/MA5608T in VDSL IPoE mode.

Copyright © Huawei Technologies Co., Ltd.

Figure 3-7 Example network of the multicast service



Data Plan

Table 3-1 lists the data plan for configuring the multicast video service with static program configuration.

Table 3-1 Data plan for configuring the multicast video service with static program configuration

Item	Data
Multicast VLAN	Multicast domain of ISP 1: VLAN 10 Multicast domain of ISP 2: VLAN 20 **NOTE** It is recommended that different multicast VLANs be planned for different ISPs.
Multicast upstream port	0/19/0
Multicast mode	IGMP proxy
Multicast protocol	IGMPv3

Copyright © Huawei Technologies Co., Ltd.

Item	Data
Multicast program	ISP 1 ● Program source address: 10.10.10.10 ● program1: 224.1.1.1 ● program2: 224.1.1.2 ● Maximum program bandwidth: 3500 kbit/s ● Program log reporting: enabled ISP 2 ● Program source address: 10.10.10.11 ● program3: 224.1.1.3 ● program4: 224.1.1.4 ● Maximum program bandwidth: 5000 kbit/s ● Program log reporting: enabled
Right profile	Music program ● Profile name: music ● Program right: watch Video program ● Profile name: movie ● Program right: watch
VDSL port attribute	Working mode: PTM Bound line profile and alarm profile: default profiles (profile ID: 1) Port connected to user 1: 0/2/1 Port connected to user 2: 0/4/1
Multicast user	User 1: ● Name of the bound right profile: music ● Maximum multicast bandwidth: 10 Mbit/s ● Multicast user log recording: enabled User 2: ● Name of the bound right profile: movie ● Maximum multicast bandwidth: 5 Mbit/s ● Multicast user log recording: enabled

Procedure

Step 1 Configure multicast VLANs and programs.

Configure smart VLAN 10 as the multicast domain of ISP 1, and smart VLAN 20 as the multicast domain of ISP 2.

Copyright © Huawei Technologies Co., Ltd.

1. Configure the protocol, multicast upstream port, and program list of multicast VLAN 10.

   Set the multicast VLAN to VLAN 10, multicast mode to IGMP proxy, multicast protocol to IGMPv3 (system default), multicast upstream port to port 0/19/0, statically configured programs to 224.1.1.1 and 224.1.1.2, program source address to 10.10.10.10, and program bandwidth to 3500 kbit/s, and enable program log reporting.

```
huawei(config)#vlan 10 smart
huawei(config)#multicast-vlan 10
huawei(config-mvlan10)#igmp mode proxy
huawei(config-mvlan10)#igmp uplink-port 0/19/0
huawei(config-mvlan10)#igmp program add name program1 ip 224.1.1.1 sourceip
10.10.10.10
 bandwidth 3500 log enable
huawei(config-mvlan10)#igmp program add name program2 ip 224.1.1.2 sourceip
10.10.10.10
 bandwidth 3500 log enable
huawei(config-mvlan10)#quit
```

2. Configure the multicast protocol, multicast upstream port, and program list of multicast VLAN 20.

   Set the multicast VLAN to VLAN 20, multicast mode to IGMP proxy, multicast protocol to IGMPv3 (system default), multicast upstream port to port 0/19/0, statically configured programs to 224.1.1.3 and 224.1.1.4, program source address to 10.10.10.11, and program bandwidth to 5000 kbit/s, and enable program log reporting.

```
huawei(config)#vlan 20 smart
huawei(config)#multicast-vlan 20
huawei(config-mvlan20)#igmp mode proxy
huawei(config-mvlan20)#igmp uplink-port 0/19/0
huawei(config-mvlan20)#igmp program add name program3 ip 224.1.1.3 sourceip
10.10.10.11
 bandwidth 5000 log enable
huawei(config-mvlan20)#igmp program add name program4 ip 224.1.1.4 sourceip
10.10.10.11
 bandwidth 5000 log enable
```

Step 2 Configure right profiles named **music** and **movie** with the watch right, and bind the right profiles to the programs.

```
huawei(config-mvlan20)#btv
huawei(config-btv)#igmp profile add profile-name music
huawei(config-btv)#igmp profile profile-name music program-name program1 watch
huawei(config-btv)#igmp profile profile-name music program-name program2 watch
huawei(config-btv)#igmp profile profile-name music program-name program3 watch
huawei(config-btv)# igmp profile add profile-name movie
huawei(config-btv)#igmp profile profile-name movie program-name program4 watch
huawei(config-btv)#quit
```

Step 3 Activate the VDSL ports, and bind the ports to the line profile and alarm profile.

Bind VDSL port 0/2/1 and VDSL port 0/4/1 to the default line profile (line profile 1) and the default alarm profile (alarm profile 1).

```
huawei(config)#interface vdsl 0/2
huawei(config-if-vdsl-0/2)#deactivate 1
huawei(config-if-vdsl-0/2)#activate 1 template-index 1
huawei(config-if-vdsl-0/2)#alarm-config 1 1
huawei(config-if-vdsl-0/2)#quit
huawei(config)#interface vdsl 0/4
huawei(config-if-vdsl-0/4)#deactivate 1
huawei(config-if-vdsl-0/4)#activate 1 template-index 1
huawei(config-if-vdsl-0/4)#alarm-config 1 1
huawei(config-if-vdsl-0/4)#quit
```

Step 4 Configure multicast users.

Copyright © Huawei Technologies Co., Ltd.

1. Create the service channels of the multicast users.

   Create service port 100 on VDSL port 0/2/1, and service port 101 on VDSL port 0/4/1.

   ```
   huawei(config)#port vlan 10 0/19 0
   huawei(config)#port vlan 20 0/19 0
   huawei(config)#service-port 100 vlan 10 vdsl mode ptm 0/2/1 rx-cttr 2 tx-cttr
   2
   huawei(config)#service-port 101 vlan 20 vdsl mode ptm 0/4/1 rx-cttr 2 tx-cttr
   2
   ```

2. Configure the attributes of the multicast users.

   Configure multicast user 0/2/1 as the authentication type, with log reporting enabled, and with the maximum bandwidth 10 Mbit/s. Configure multicast user 0/4/1 as the authentication type, with log reporting enabled, and with the maximum bandwidth 5 Mbit/s.

   ```
   huawei(config)#btv
   huawei(config-btv)#igmp user add service-port 100 auth log enable max-
   bandwidth 10240
   huawei(config-btv)#igmp user add service-port 101 auth log enable max-
   bandwidth 5120
   ```

3. Bind the multicast users to the right profiles.

   Bind VDSL user 0/2/1 to right profile **music**, and VDSL user 0/4/1 to right profile **movie**.

   ```
   huawei(config-btv)#igmp user bind-profile service-port 100 profile-name music
   huawei(config-btv)#igmp user bind-profile service-port 101 profile-name movie
   ```

4. Add the VDSL users to the multicast VLANs so that the VDSL users are multicast members.

   ```
   huawei(config-btv)#multicast-vlan 10
   huawei(config-mvlan10)#igmp multicast-vlan member service-port 100
   huawei(config-mvlan10)#multicast-vlan 20
   huawei(config-mvlan20)#igmp multicast-vlan member service-port 101
   huawei(config-mvlan20)#quit
   ```

Step 5 Save the configuration.

```
huawei(config)#save
```

----End

Result

- VDSL user 0/1/0 can watch the programs with IP addresses 224.1.1.1 and 224.1.1.2 that are provided by ISP 1, but VDSL user 0/1/0 cannot watch the program with IP address 224.1.1.3.
- VDSL user 0/2/0 can watch the program with IP address 224.1.1.4 that is provided by ISP 2.

Configuration File

```
vlan 10 smart
multicast-vlan 10
igmp mode proxy
igmp uplink-port 0/19/0
igmp program add name program1 ip 224.1.1.1 sourceip 10.10.10.10
 bandwidth 3500 log enable
igmp program add name program2 ip 224.1.1.2 sourceip 10.10.10.10
 bandwidth 3500 log enable
```


Copyright © Huawei Technologies Co., Ltd.

```
quit
vlan 20 smart
igmp mode proxy
igmp uplink-port 0/19/0
igmp program add name program3 ip 224.1.1.3 sourceip 10.10.10.11
 bandwidth 5000 log enable
igmp program add name program4 ip 224.1.1.4 sourceip 10.10.10.11
 bandwidth 5000 log enable
btv
igmp profile add profile-name music
igmp profile profile-name music program-name program1 watch
igmp profile profile-name music program-name program2 watch
igmp profile profile-name music program-name program3 watch
igmp profile add profile-name movie
igmp profile profile-name movie program-name program4 watch
quit
interface vdsl 0/2
deactivate 1
activate 1 template-index 1
alarm-config 1 1
quit
interface vdsl 0/4
deactivate 1
activate 1 template-index 1
alarm-config 1 1
quit
port vlan 10 0/19 0
port vlan 20 0/19 0
service-port 100 vlan 10 vdsl mode ptm 0/2/1 rx-cttr 2 tx-cttr 2
service-port 101 vlan 20 vdsl mode ptm 0/4/1 rx-cttr 2 tx-cttr 2
btv
igmp user add service-port 100 auth log enable max-bandwidth 10240
igmp user add service-port 101 auth log enable max-bandwidth 5120
igmp user bind-profile service-port 100 profile-name music
igmp user bind-profile service-port 101 profile-name movie
multicast-vlan 10
igmp multicast-vlan member service-port 100
multicast-vlan 20
igmp multicast-vlan member service-port 101
quit
save
```

3.2.2 Configuration Example of the Multicast Video Service (Dynamic Program Generation)

Dynamic program generation simplifies multicast service configuration and reduces maintenance cost, but does not support functions of program/user multicast bandwidth management, program preview, and program prejoin. This configuration mode applies to multicast services that do not have strict requirements on program and user management or to those having programs and users managed on the upper-layer device.

Service Requirements

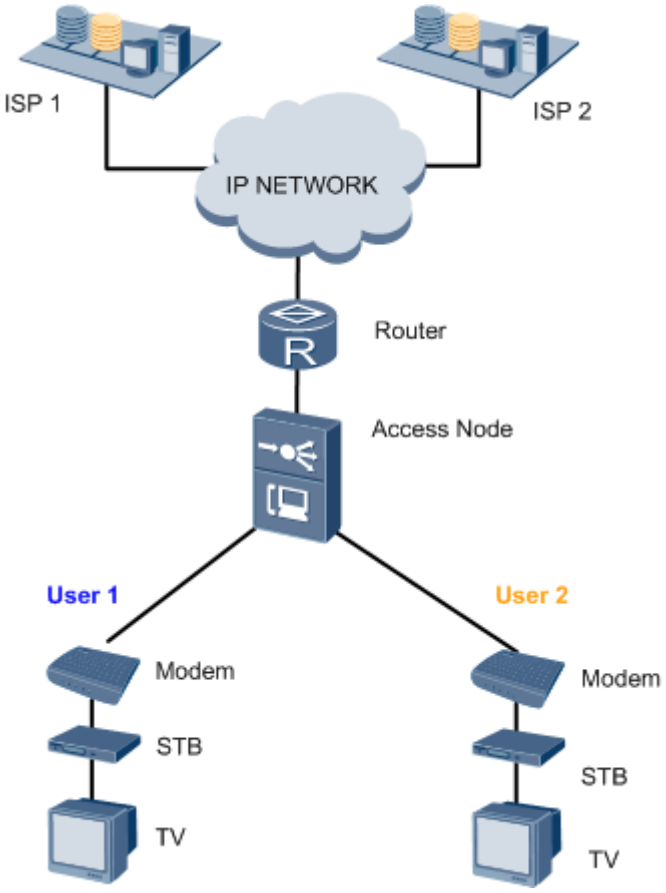
- ISP 1 and ISP 2 each have an address segment corresponding to multicast programs, which do not require strict management and are dynamically updated according to the ordering situation.
- The service package purchased by user 1 allows user 1 to watch programs of ISP 1 only. The service package purchased by user 2 allows user 2 to watch programs of ISP 2 only.
- The ordering information about users can be recorded for monitoring and charging.

Figure 3-8 shows an example network of the multicast service.

Copyright © Huawei Technologies Co., Ltd.

User 1 and user 2 are connected to the MA5600T/MA5603T/MA5608T in VDSL IPoE mode.

Figure 3-8 Example network of the multicast service



Data Plan

Table 3-2 lists the data plan for configuring the multicast video service with dynamic program generation.

Table 3-2 Data plan for configuring the multicast video service with dynamic program generation

Item	Data
Multicast VLAN	Multicast domain of ISP 1: VLAN 10 Multicast domain of ISP 2: VLAN 20 **NOTE** It is recommended that different multicast VLANs be planned for different ISPs.
Multicast upstream port	0/19/0
Multicast mode	IGMP proxy

Copyright © Huawei Technologies Co., Ltd.

Item	Data
Multicast protocol	IGMPv3
Multicast program	Dynamic generation Program address range of ISP 1: 224.1.1.1-224.1.1.2 Program address range of ISP 2: 224.1.1.3-224.1.1.4
VDSL port attribute	Working mode: PTM Bound line profile and alarm profile: default profiles (profile ID: 1) Port connected to user 1: 0/2/1 Port connected to user 2: 0/4/1
Multicast user	Multicast user log recording: enabled

Procedure

Step 1 Configure multicast VLANs and programs.

Configure smart VLAN 10 as the multicast domain of ISP 1, and smart VLAN 20 as the multicast domain of ISP 2.

1. Configure the protocol, multicast upstream port, and program list of multicast VLAN 10.

   Configure multicast VLAN 10 with the dynamic program generation mode, and specify the range of the IP addresses of the programs that can be requested by the users in multicast VLAN 10 as 224.1.1.1 to 224.1.1.2. Multicast VLAN 10 adopts IGMP proxy, IGMP v3 (system default value), and multicast upstream port 0/19/0.

   NOTICE

   The multicast program configuration mode can be changed only when **igmp match mode** is set to **off**. However, setting **igmp match mode** to **off** will cause users to go offline. Therefore, it is recommended that the program configuration mode be planned beforehand.

   ```
   huawei(config)#vlan 10 smart
   huawei(config)#multicast-vlan 10
   huawei(config-mvlan10)#igmp match mode disable
   huawei(config-mvlan10)#igmp match group ip 224.1.1.1 to-ip 224.1.1.2
   huawei(config-mvlan10)#igmp uplink-port 0/19/0
   huawei(config-mvlan10)#igmp mode proxy
   huawei(config-mvlan10)#quit
   ```

2. Configure the protocol, multicast upstream port, and program list of multicast VLAN 20.

   Configure multicast VLAN 20 with the dynamic program generation mode, and specify the range of the IP addresses of the programs that can be requested by the users in multicast VLAN 10 as 224.1.1.3 to 224.1.1.4. Multicast VLAN 20 adopts IGMP proxy, IGMP v3 (system default value), and multicast upstream port 0/19/0.

   ```
   huawei(config)#vlan 20 smart
   huawei(config)#multicast-vlan 20
   huawei(config-mvlan20)#igmp match mode disable
   ```


Copyright © Huawei Technologies Co., Ltd.

```
huawei(config-mvlan20)#igmp match group ip 224.1.1.3 to-ip 224.1.1.4
huawei(config-mvlan20)#igmp uplink-port 0/19/0
huawei(config-mvlan20)#igmp mode proxy
huawei(config-mvlan20)#quit
```

Step 2 Activate the VDSL ports, and bind the ports to the line profile and alarm profile.

Bind VDSL port 0/2/1 and VDSL port 0/4/1 to the default line profile (line profile 1) and the default alarm profile (alarm profile 1).

```
huawei(config)#interface vdsl 0/2
huawei(config-if-vdsl-0/2)#deactivate 1
huawei(config-if-vdsl-0/2)#activate 1 template-index 1
huawei(config-if-vdsl-0/2)#alarm-config 1 1
huawei(config-if-vdsl-0/2)#quit
huawei(config)#interface vdsl 0/4
huawei(config-if-vdsl-0/4)#deactivate 1
huawei(config-if-vdsl-0/4)#activate 1 template-index 1
huawei(config-if-vdsl-0/4)#alarm-config 1 1
huawei(config-if-vdsl-0/4)#quit
```

Step 3 Configure multicast users.

1. Create the service channels of the multicast users.

   Create service port 100 on VDSL port 0/2/1, and service port 101 on VDSL port 0/4/1.

   ```
   huawei(config)#port vlan 10 0/19 0
   huawei(config)#port vlan 20 0/19 0
   huawei(config)#service-port 100 vlan 10 vdsl mode ptm 0/2/1 rx-cttr 2 tx-cttr
   2
   huawei(config)#service-port 101 vlan 20 vdsl mode ptm 0/4/1 rx-cttr 2 tx-cttr
   2
   ```

2. Configure the attributes of the multicast users.

   Enable the log reporting for multicast users 0/2/1 and 0/4/1. The authentication status and multicast bandwidth of the multicast users do not need to be configured.

   ```
   huawei(config)#btv
   huawei(config-btv)#igmp user add service-port 100 log enable
   huawei(config-btv)#igmp user add service-port 101 log enable
   huawei(config-btv)#quit
   ```

3. Add the VDSL users to the multicast VLANs so that the VDSL users are multicast members.

   ```
   huawei(config)#multicast-vlan 10
   huawei(config-mvlan10)#igmp multicast-vlan member service-port 100
   huawei(config-mvlan10)#quit
   huawei(config-btv)#multicast-vlan 20
   huawei(config-mvlan20)#igmp multicast-vlan member service-port 101
   huawei(config-mvlan20)#quit
   ```

Step 4 Save the configuration.

```
huawei(config)#save
```

----End

Result

- VDSL user 0/2/1 can watch the programs with IP addresses 224.1.1.1 and 224.1.1.2 that are provided by ISP 1.
- VDSL user 0/4/1 can watch the programs with IP addresses 224.1.1.3 and 224.1.1.4 that are provided by ISP 2.

Copyright © Huawei Technologies Co., Ltd.

Configuration File

```
vlan 10 smart
multicast-vlan 10
igmp match mode disable
igmp match group ip 224.1.1.1 to-ip 224.1.1.2
igmp uplink-port 0/19/0
igmp mode proxy
quit
vlan 20 smart
igmp match mode disable
igmp match group ip 224.1.1.3 to-ip 224.1.1.4
igmp uplink-port 0/19/0
igmp mode proxy
quit
interface vdsl 0/2
deactivate 1
activate 1 template-index 1
alarm-config 1 1
quit
interface vdsl 0/4
deactivate 1
activate 1 template-index 1
alarm-config 1 1
quit
port vlan 10 0/19 0
port vlan 20 0/19 0
service-port 100 vlan 10 vdsl mode ptm 0/2/1 rx-cttr 2 tx-cttr 2
service-port 101 vlan 20 vdsl mode ptm 0/4/1 rx-cttr 2 tx-cttr 2
btv
igmp user add service-port 100 auth log enable
igmp user add service-port 101 auth log enable
multicast-vlan 10
igmp multicast-vlan member service-port 100
multicast-vlan 20
igmp multicast-vlan member service-port 101
quit
save
```

3.3 Example: Configuring the VoIP Service

This topic describes how to configure the H.248-based, MGCP-based, and SIP-based VoIP services respectively.

3.3.1 Example: Configuring the VoIP Service (H.248-based)

This topic describes an example for configuring the H.248-based VoIP service.

Service Requirements

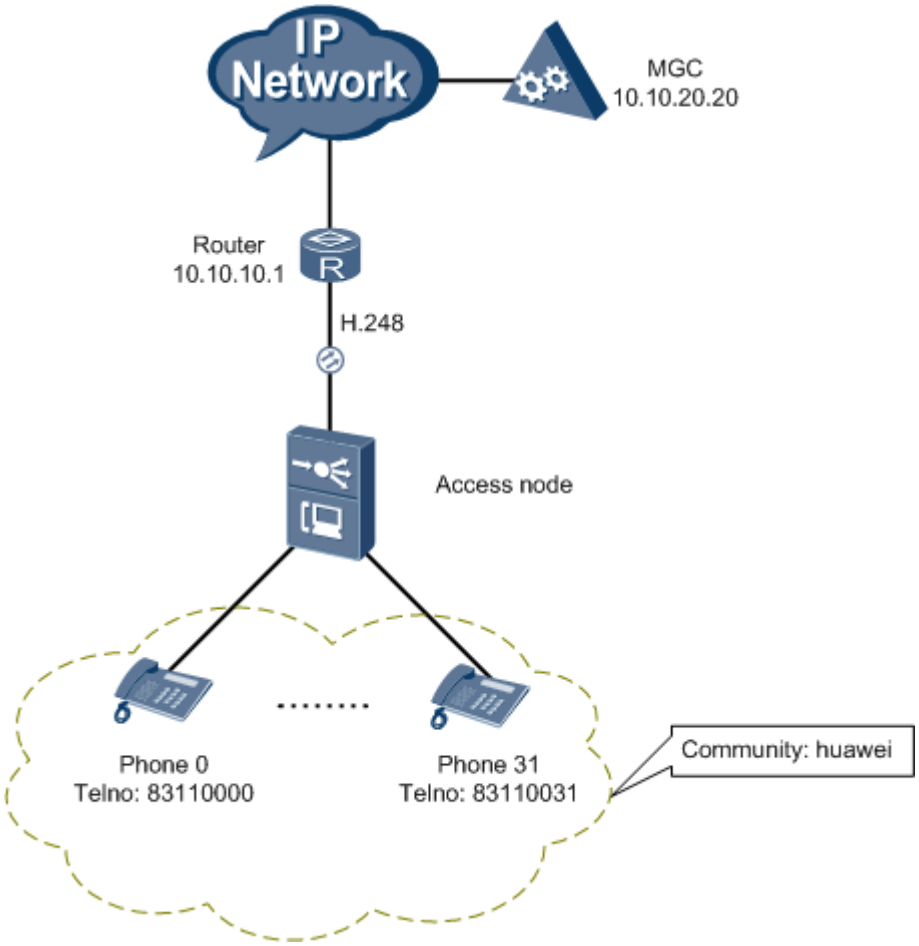
In an office located in China, the MA5600T/MA5603T/MA5608T that adopts the H.248 protocol is newly deployed. Data plan and configuration, however, are not performed on the MGC (softswitch) connected to the MA5600T/MA5603T/MA5608T. The MA5600T/MA5603T/MA5608T is required to provide the following VoIP services:

- The common phone services are provisioned to 32 users (phones 0-31).
- The polarity-reversal accounting is adopted.

Figure 3-9 shows an example network for configuring the H.248-based VoIP service.

Copyright © Huawei Technologies Co., Ltd.

Figure 3-9 Example network for configuring the H.248-based VoIP service



Prerequisite

- According to the actual network, a route from the MA5600T/MA5603T/MA5608T to the MGC must be configured to ensure that the MA5600T/MA5603T/MA5608T and the MGC are reachable from each other.
- Electronic switch 0 must be in **location-1** (indicating that the system goes upstream through only the upstream board). Electronic switch 1 must be in **location-0** (indicating that the VoIP service is supported). For details about how to configure the electronic switch, see **electro-switch**.

  NOTE

  - The SCUN and SCUH control boards do not support electronic switch.
  - The control board SCUL does not provide the upstream port and the system goes upstream through only the upstream board.

Data Plan

After the service requirements are further confirmed and analyzed with the service provider, the data plan is made by considering the interconnection with the MGC and according to the data plan described in Configuring the VoIP Service (H.248-based or MGCP-based). **Table 3-3** provides the data plan for configuring the H.248-based VoIP service.

Copyright © Huawei Technologies Co., Ltd.

Table 3-3 Data plan for configuring the H.248-based VoIP service

Item			Data
MG interface data (The data configuration on the MG interface must be the same as the data configuration on the MGC.)	Media and signaling parameters	Media and signaling upstream VLAN	Standard VLAN is recommended as the upstream VLAN of the VoIP service. Standard VLAN 20 is adopted.
		Media and signaling upstream port	In this office, all the services are transmitted upstream through the upstream interface board. Therefore, port 0/19/0 is used as the upstream port of the VoIP service.
		Media and signaling IP addresses	These two IP addresses are both 10.10.10.10.
		Default IP address of the MG	Confirmed with the engineers of this service provider, the next hop IP address from MA5600T/MA5603T/MA5608T to the MGC is 10.10.10.1.
	Parameters of the MG interface **NOTE** Parameters listed here are mandatory, which means that the MG interface fails to be enabled if these parameters are not configured.	MG interface ID	Confirmed with the engineers of this service provider, the 32 users to be provisioned with the services are the first batch of users in the community named **huawei**, and later other users in this community will be provisioned with the same services gradually. The number of users in this community is 10,000. Considering that the number of users is large, the office assigns a VAG (VAG 0) to this community for better management. Therefore, the MG interface ID is 0
		Signaling port ID of the MG interface	The signaling port ID is 2944.
		IP address of the primary MGC to which the MG interface belongs	The service provider does not provide dual homing for its network. According to the network topology, the IP address of the primary MGC is 10.10.20.20, and the port ID is 2944, the same as the port ID on the MA5600T/MA5603T/MA5608T.
		Port ID of the primary MGC to which the MG interface belongs	
		Coding mode of the MG interface	The **text** coding mode is adopted.

Copyright © Huawei Technologies Co., Ltd.

Item			Data
		Transmission mode of the MG interface	UDP is adopted.
		Domain name of the MG interface	The message ID (MID) adopts the IP address (default), and may not be configured with the domain name.
	Digitmap of the MG interface		Special applications such as emergency calls and emergency standalone are not configured, and therefore the digitmap is not configured here.
	Software parameters of the MG interface		According to the Background Information in (Optional) Configuring the Software Parameters of an MG Interface and confirmed with the service provider, the default settings can meet the service requirements. Therefore, the software parameters are not configured here.
	Ringing mode of the MG interface		Confirmed with the service provider, the value of the ringing parameter (corresponding to the users) defined on the MGC is 0 (value of *mgcpara*), and the users have no special requirements for the ringing mode. Therefore, the normal ringing with the break-make ratio of 1:4 is adopted.
	Terminal ID (TID) format of the MG interface		To differentiate users according to the TID, the service provider requires that the terminal prefix uses the community name **huawei** and the TID is automatically generated by the system according to the slot ID/subrack ID/port ID of the user. Run the **display tid-template** command to query the default TID template. It is found that default TID template (template 6) can meet the requirements.
VoIP user data (The data configuration must be the same as the data	Slot for the voice service board		User access is implemented by the ASPB board in slot 0/3.

Copyright © Huawei Technologies Co., Ltd.

Item			Data
configuration on the MGC.)	User data	Phone number	The emergency standalone is not supported, and therefore the configuration of phone numbers is not required when the users are added. The MGC assigns phone numbers 83110000-83110031 to phones 0-31 respectively.
		TID	The terminal layering is supported, and therefore the manual allocation of TIDs is not required.
		User priority	The users are common users, and the user priority uses the default cat3.
		User type	The users are common users, and the users are of the default DEL type.
	System parameters		According to the Background Information in (Optional) Configuring the System Parameters and confirmed with the service provider, the default settings can meet the service requirements. Therefore, the system parameters are not configured here.
	Overseas parameters		According to the Background Information in (Optional) Configuring the Overseas Parameters and confirmed with the service provider, the default settings can meet the service requirements. Therefore, the overseas parameters are not configured here.
	PSTN port attributes		The polarity reversal accounting is adopted, and therefore the PSTN port to which the users belong needs to support the polarity reversal pulse. The other attributes of the PSTN port do not need to be modified.
	Ringing current attributes		There is no special requirement, and the configuration of the ringing current attributes is not required.

Procedure

Step 1 Add the upstream VLAN interface.

According to the data plan, configure standard VLAN 20 as the media and signaling upstream VLAN, add upstream port 0/19/0 to the VLAN, and configure the IP address of the Layer 3

Copyright © Huawei Technologies Co., Ltd.

interface to 10.10.10.10, which facilitates the configuration of the media and signaling IP address pools.

```
huawei(config)#vlan 20 standard
huawei(config)#port vlan 20 0/19 0
huawei(config)#interface vlanif 20
huawei(config-if-vlanif20)#ip address 10.10.10.10 24
huawei(config-if-vlanif20)#quit
```

Step 2 Configure the media and signaling IP address pools.

Add the IP address of the VLAN Layer 3 interface configured in the previous step to the media and signaling IP address pools respectively, which facilitates the selection of media and signaling IP addresses used for the services from the IP address pools. According to the data plan, IP address 10.10.10.10 is added to the media and signaling IP address pools, and the gateway IP address corresponding to the media IP address is 10.10.10.1.

```
huawei(config)#voip
huawei(config-voip)#ip address media 10.10.10.10 10.10.10.1
huawei(config-voip)#ip address signaling 10.10.10.10
huawei(config-voip)#quit
```

NOTE

- You can configure the attributes of the H248 or MG interface only when the media IP address and the signaling IP address exist in the media and signaling IP address pools.
- The media IP address and the signaling IP address can be different. You can plan the IP addresses according to the actual network.

Step 3 Add an MG interface.

Add an MG interface to communicate with the MGC, which ensures that the MGC can control the call connection through the MG interface. According to the data plan, add MG interface 0, and configure the interface attributes.

```
huawei(config)#interface h248 0
  Are you sure to add MG interface?(y/n)[n]:y
huawei(config-if-h248-0)#if-h248 attribute mg-media-ip1 10.10.10.10 mgip
10.10.10.10 mgport 2944 primary-mgc-ip1 10.10.20.20
primary-mgc-port 2944 code text transfer udp
```

Step 4 Configure the ringing mapping of MG interface 0.

Configure the user ringing mode. According to the data plan, the break-make ratios of the cadence ringing and the initial ringing are both 1:4. Therefore, the value of parameter *cadence* is 0, and the value of parameter *initialring* is 4.

```
huawei(config-if-h248-0)#mg-ringmode add 0 0 4
```

Step 5 Configure the TID format of PSTN users on MG interface 0.

Configure the TID generation mode. According to the data plan, the terminal prefix of PSTN users needs to be **huawei**, and the TID template adopts layering template 6.

NOTICE

The MA5600T/MA5603T/MA5608T requires that the terminal prefixes of PSTN users, ISDN BRA users, and ISDN PRA users on the same H.248 interface are either the same or different. Note this when configuring the terminal prefix.

Copyright © Huawei Technologies Co., Ltd.

```
huawei(config-if-h248-0)#tid-format pstn prefix huawei template 6
```

Step 6 Enable the MG interface.

Reset the MG interface to make the MG interface register with the MGC (or to make the attributes of the MG interface take effect), so that the MG interface can work in the normal state. The MG interface can be enabled in different ways (see Parameters of the **reset** command). For a newly configure MG interface, enable the MG interface through cold start.

```
huawei(config-if-h248-0)#reset coldstart
  Are you sure to reset MG interface?(y/n)[n]:y
huawei(config-if-h248-0)#quit
```

Step 7 Query the running status of the MG interface.

After the MG interface is interconnected with the MGC, the MG interface should be in the normal state, indicating that the MG interface can work in the normal state.

```
huawei(config)#display if-h248 all
  ------------------------------------------------------------------------
  MGID   TransMode State    MGPort MGIP/DomainName MGCPort MGCIP/DomainName
  ------------------------------------------------------------------------
  0      UDP       Normal   2944   10.10.10.10     2944    10.10.20.20
  ------------------------------------------------------------------------
```

Step 8 Confirm the service board.

Confirm the ASPB board that carries services to ensure that the board can work in the normal state.

```
huawei(config)#board confirm 0/3
```

Step 9 Configure the PSTN user data.

Add POTS users (phones 0-31) to ensure that users can go online.

```
huawei(config)#esl user
huawei(config-esl-user)#mgpstnuser batadd 0/3/0 0/3/31 0
huawei(config-esl-user)#quit
```

Step 10 Configure the polarity reversal accounting function.

Configure the physical attributes of the PSTN port to which the users belong to support the polarity reversal pulse, so that the users can support the polarity reversal accounting.

```
huawei(config)#pstnport
huawei(config-pstnport)#pstnport attribute batset 0/3/0 0/3/31 reverse-pole-pulse
enable
huawei(config-pstnport)#quit
```

Step 11 Save the data.

```
huawei(config)#save
```

----End

Result

After the interface data and the PSTN user data corresponding to the MG interface are configured on the MGC, check whether the VoIP services can be provisioned normally. In the normal state, phones 0-31 can make phone calls to each other:

- The caller can hear the dial tone after picking up the phone.

Copyright © Huawei Technologies Co., Ltd.

- When the caller dials the phone number of the callee, the phone of the callee can ring normally, and the caller can hear the ring back tone.
- The caller and the callee can communicate with each other successfully.
- After the callee hangs up the phone, the caller can hear the busy tone.

Configuration File

The following describes the configuration file of this configuration example. Note that certain steps must be performed manually and the configuration file cannot be imported directly.

Configure the upstream VLAN interface.

```
vlan 20 standard
port vlan 20 0/19 0
interface vlanif 20
ip address 10.10.10.10 24
quit
```

Configure the media and signaling IP address pools.

```
voip
ip address media 10.10.10.10 10.10.10.1
ip address signaling 10.10.10.10
quit
```

Add an MG interface and configure the attributes of the MG interface. The MG interface must be configured manually, and the configuration profile cannot be directly imported.

```
interface h248 0
if-h248 attribute mg-media-ip1 10.10.10.10 mgip 10.10.10.10 mgport 2944 primary-
mgc-ip1 10.10.20.20
 primary-mgc-port 2944 code text transfer udp
```

Configure the ringing mapping of the MG interface.

```
mg-ringmode add 0 0 4
```

Configure the TID format of the PSTN user on the MG interface.

```
tid-format pstn prefix huawei template 6
```

Enable the MG interface. The MG interface must be enabled manually, and the configuration profile cannot be directly imported.

```
reset coldstart
quit
```

Query the running status of the MG interface.

```
display if-h248 all
```

Confirm the service board.

```
board confirm 0/3
```

Configure the PSTN user data.

```
esl user
mgpstnuser batadd 0/3/0 0/3/31 0
quit
```

Configure the polarity reversal accounting function.

Copyright © Huawei Technologies Co., Ltd.

```
pstnport
pstnport attribute batset 0/3/0 0/3/31 reverse-pole-pulse enable
quit
```

Save the data.

```
save
```

3.3.2 Example: Configuring the VoIP Service (MGCP-based)

This topic describes how to configure the MGCP-based VoIP service.

Service Requirements

In an office located in China, the MA5600T/MA5603T/MA5608T that adopts the MGCP protocol is newly deployed. Data plan and configuration, however, are not performed on the MGC (softswitch) connected to the MA5600T/MA5603T/MA5608T. The MA5600T/MA5603T/MA5608T is required to provide the following VoIP services:

- The common phone services are provisioned to 32 users (phones 0-31).
- The polarity-reversal accounting is adopted.

After the service requirements are further confirmed and analyzed with the service provider, the data plan is made by considering the interconnection with the MGC and according to the data plan described in Configuring the VoIP Service (H.248-based or MGCP-based). **Table 3-4** provides the data plan for configuring the MGCP-based VoIP service.

Table 3-4 Data plan for configuring the MGCP-based VoIP service

Item			Data
MG interface data (The data configuration must be the same as the data configuration on the MGC.)	Media and signaling parameters	Media and signaling upstream VLAN	Standard VLAN is recommended as the upstream VLAN of the VoIP service. Standard VLAN 20 is adopted.
		Media and signaling upstream port	In this office, all the services are transmitted upstream through the upstream interface board. Therefore, port 0/19/0 is used as the upstream port of the VoIP service.
		Media and signaling IP address	These two IP addresses are both 10.10.10.10/24. **NOTICE** The MGCP interface on the MA5600T/MA5603T/MA5608T does not support the isolation of media streams and signaling flows. Therefore, when the MGCP protocol is used, the media IP address pool and the signaling IP address pool must be the same. When the H.248 or SIP protocol is used, the media IP address pool and the signaling IP address pool can be the same or different.

Copyright © Huawei Technologies Co., Ltd.

Item			Data
		Default IP address of the gateway	Confirmed with the engineers of this service provider, the next hop IP address from MA5600T/MA5603T/ MA5608T to the MGC is 10.10.10.1.
	Parameters of the MG interface **NOTE** Parameters listed here are mandatory, which means that the MG interface fails to be enabled if these parameters are not configured.	MG interface ID	Confirmed with the engineers of this service provider, the 32 users to be provisioned with the services are the first batch of users in the community named **huawei**, and later other users will be provisioned with the same services gradually. The number of users in this community is 10,000. Considering that the number of users is large, the service provider assigns a VAG (VAG 0) to this community for better management. Therefore, the MG interface ID is 0.
		Signaling port ID of the MG interface	The signaling port ID is 2727.
		IP address of the primary MGC to which the MG interface belongs	The service provider does not provide dual homing for its network. According to the network topology, the IP address of the primary MGC is 10.10.20.20, and the port ID is 2727, the same as the port ID on the MA5600T/MA5603T/MA5608T.
		Port ID of the primary MGC to which the MG interface belongs	
		Coding mode of the MG interface	For the MG interface that supports MGCP, the default coding mode is the **text** coding mode. This parameter can be queried, but cannot be configured.
		Transmission mode of the MG interface	For the MG interface that supports MGCP, the default transmission mode is UDP. This parameter can be queried, but cannot be configured.
		Domain name of the MG interface	The community name **huawei** is adopted.
	Digitmap of the MG interface		Special applications such as emergency calls and emergency standalone are not configured, and therefore the digitmap is not configured.

Copyright © Huawei Technologies Co., Ltd.

Item			Data
	Software parameters of the MG interface		According to the Background Information in (Optional) Configuring the Software Parameters of an MG Interface and confirmed with the service provider, the default settings can meet the service requirements. Therefore, the software parameters are not configured here.
	Ringing mode of the MG interface		Confirmed with the service provider, the value of the ringing parameter (corresponding to the users) defined on the MGC is 0 (value of *mgcpara*), and the users have no special requirements for the ringing mode. Therefore, the normal ringing with the break-make ratio of 1:4 is adopted.
	Terminal ID (TID) format of the MG interface		To differentiate users according to the TID, the service provider requires that the terminal prefix uses the community name **huawei** and the TID is automatically generated by the system according to the slot ID/subrack ID/ port ID of the user. Run the **display tid-template** command to query the default TID template. It is found that default TID template 6 can meet the requirements.
VoIP user data (The data configuration must be the same as the data configuration on the MGC.)	Slot of the voice service board		User access is implemented by the ASPB board in slot 0/3.
	User data	Phone number	MGCP does not support emergency standalone, and therefore the phone number does not need to be configured when the user is added. The MGC assigns phone numbers 83110000-83110031 to phones 0-31 respectively.
		TID	The terminal layering is supported, and therefore the manual allocation of TIDs is not required.
		User priority	The users are common users, and the user priority uses default cat3.
		User type	The users are common users, and the users are of the default DEL type.

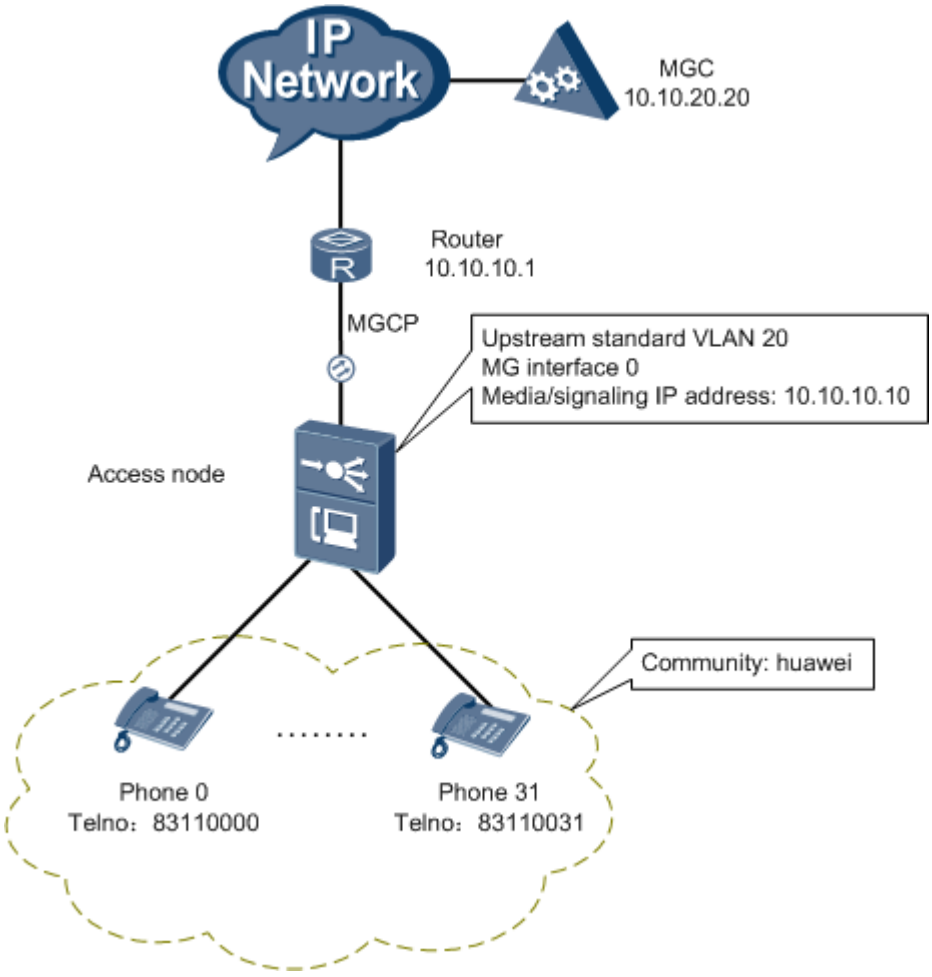
Copyright © Huawei Technologies Co., Ltd.

Item		Data
	System parameters	According to the Background Information in (Optional) Configuring the System Parameters and confirmed with the service provider, the default settings can meet the service requirements. Therefore, the system parameters are not configured here.
	Overseas parameters	According to the Background Information in (Optional) Configuring the Overseas Parameters and confirmed with the service provider, the default settings can meet the service requirements. Therefore, the overseas parameters are not configured here.
	PSTN port attributes	The polarity reversal accounting is adopted, and therefore the PSTN port to which the users belong needs to support the polarity reversal pulse. The other attributes of the PSTN port do not need to be modified.
	Ringing current attributes	There is no special requirement, and the configuration of the ringing current attributes is not required.

Figure 3-10 shows an example network for configuring the MGCP-based VoIP service.

Copyright © Huawei Technologies Co., Ltd.

Figure 3-10 Example network for configuring the MGCP-based VoIP service



Prerequisite

- According to the actual network, a route from the MA5600T/MA5603T/MA5608T to the MGC must be configured to ensure that the MA5600T/MA5603T/MA5608T and the MGC are reachable from each other.
- Electronic switch 0 must be in **location-1** (indicating that the system goes upstream through only the upstream board). Electronic switch 1 must be in **location-0** (indicating that the VoIP service is supported). For details about how to configure the electronic switch, see **electro-switch**.

  NOTE

  - The SCUN and SCUH control boards do not support electronic switch.
  - The control board SCUL does not provide the upstream port and the system goes upstream through only the upstream board.
- The POTS service board, namely the ASPB board, must be inserted into the planned slot, and the RUN ALM LED of the board must be green and must be on for 1s and off for 1s repeatedly.

Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Add the upstream VLAN interface.

According to the data plan, configure standard VLAN 20 as the media and signaling upstream VLAN, add upstream port 0/19/0 to the VLAN, and configure the IP address of the Layer 3 interface to 10.10.10.10, which facilitates the configuration of the media and signaling IP address pools.

```
huawei(config)#vlan 20 standard
huawei(config)#port vlan 20 0/19 0
huawei(config)#interface vlanif 20
huawei(config-if-vlanif20)#ip address 10.10.10.10 24
huawei(config-if-vlanif20)#quit
```

Step 2 Configure the media and signaling IP address pools.

According to the data plan, IP address 10.10.10.10 is added to the media and signaling IP address pools, and the gateway IP address corresponding to the media IP address is 10.10.10.1.

```
huawei(config)#voip
huawei(config-voip)#ip address media 10.10.10.10 10.10.10.1
huawei(config-voip)#ip address signaling 10.10.10.10
huawei(config-voip)#quit
```

Step 3 Add an MG interface.

Add an MG interface to communicate with the MGC, which ensures that the MGC can control the call connection through the MG interface. According to the data plan, add MG interface 0, and configure the interface attributes.

```
huawei(config)#interface mgcp 0
  Are you sure to add MG interface?(y/n)[n]:y
huawei(config-if-mgcp-0)#if-mgcp attribute mgip 10.10.10.10 mgport 2727 mgcip_1
10.10.20.20 mgcport_1 2727 domainName huawei
```

Step 4 Configure the ringing mapping of MG interface 0.

Configure the ringing mode of the MG interface. According to the data plan, the break-make ratios of the cadence ringing and the initial ringing are both 1:4. Therefore, the value of parameter *cadence* is 0, and the value of parameter *initialring* is 4.

```
huawei(config-if-mgcp-0)#mg-ringmode add 0 0 4
```

Step 5 Configure the TID format of PSTN users on MG interface 0.

Configure the TID generation mode. According to the data plan, the terminal prefix of PSTN users needs to be **huawei**, and the TID template adopts layering template 6.

```
huawei(config-if-mgcp-0)#tid-format pstn prefix huawei template 6
```

Step 6 Enable the MG interface.

Reset the MG interface to make the MG interface register with the MGC (or to make the attributes of the MG interface take effect), so that the MG interface can work in the normal state.

```
huawei(config-if-mgcp-0)#reset
  Are you sure to reset MG interface?(y/n)[n]:y
huawei(config-if-mgcp-0)#quit
```

Step 7 Query the running status of the MG interface.

After the MG interface is interconnected with the MGC, the MG interface should be in the normal state, indicating that the MG interface can work in the normal state.

Copyright © Huawei Technologies Co., Ltd.

```
huawei(config)#display if-mgcp all
  ------------------------------------------------------------------------
  MGID     State          MGPort MGIP            MGCPort MGCIP/DomainName
  ------------------------------------------------------------------------
  0        Normal         2727   10.10.10.10     2727    10.10.20.20
  ------------------------------------------------------------------------
```

Step 8 Configure the PSTN user data.

Add POTS users (phones 0-31) to ensure that users can go online.

```
huawei(config)#esl user
huawei(config-esl-user)#mgpstnuser batadd 0/3/0 0/3/31 0
huawei(config-esl-user)#quit
```

Step 9 Configure the polarity reversal accounting function.

Configure the physical attributes of the PSTN port to which the users belong to support the polarity reversal pulse, so that the users can support the polarity reversal accounting.

```
huawei(config)#pstnport
huawei(config-pstnport)#pstnport attribute batset 0/3/0 0/3/31 reverse-pole-pulse
enable
huawei(config-pstnport)#quit
```

Step 10 Save the data.

```
huawei(config)#save
```

----End

Result

After the interface data and the PSTN user data corresponding to the MG interface are configured on the MGC, check whether the VoIP services can be provisioned normally. In the normal state, phones 0-31 can make phone calls to each other:

- The caller can hear the dial tone after picking up the phone.
- When the caller dials the phone number of the callee, the phone of the callee can ring normally, and the caller can hear the ring back tone.
- The caller and the callee can communicate with each other successfully.
- After the callee hangs up the phone, the caller can hear the busy tone.

Configuration File

The following describes the configuration file of this configuration example. Note that certain steps must be performed manually and the configuration file cannot be imported directly.

Configure the upstream VLAN interface.

```
vlan 20 standard
port vlan 20 0/19 0
interface vlanif 20
ip address 10.10.10.10 24
quit
```

Configure the media and signaling IP address pools.

```
voip
ip address media 10.10.10.10 10.10.10.1
ip address signaling 10.10.10.10
quit
```


Copyright © Huawei Technologies Co., Ltd.

Add an MG interface and configure the attributes of the MG interface. The MG interface must be configured manually, and the configuration profile cannot be directly imported.

```
interface mgcp 0
if-mgcp attribute mgip 10.10.10.10 mgport 2727 mgcip_1 10.10.20.20 mgcport_1 2727
domainName huawei
```

Configure the ringing mapping of the MG interface.

```
mg-ringmode add 0 0 4
```

Configure the TID format of the PSTN user on the MG interface.

```
tid-format pstn prefix huawei template 6
quit
```

Enable the MG interface. The MG interface must be enabled manually, and the configuration profile cannot be directly imported.

```
reset
```

Query the running status of the MG interface.

```
display if-mgcp all
```

Confirm the service board.

```
board confirm 0/3
```

Configure the PSTN user data.

```
esl user
mgpstnuser batadd 0/3/0 0/3/31 0
quit
```

Configure the polarity reversal accounting function.

```
pstnport
pstnport attribute batset 0/3/0 0/3/31 reverse-pole-pulse enable
```

Save the data.

```
quit
save
```

3.3.3 Example: Configuring the VoIP PSTN Service (SIP)

This topic describes the configuration example of the VoIP PSTN service based on sip protocol.

Service Requirements

In an office located in China, the MA5600T/MA5603T/MA5608T that adopts the SIP protocol is newly deployed. Data plan and configuration, however, are not performed on the IMS (softswitch) connected to the MA5600T/MA5603T/MA5608T. The MA5600T/MA5603T/MA5608T is required to provide the following VoIP services:

- The common phone services are provisioned to 128 users (phones 0-127).
- The polarity-reversal accounting is adopted.

After the service requirements are further confirmed and analyzed with the office, the data plan is made by considering the interconnection with the IMS and according to the data plan described in Configuring the VoIP Service (SIP-based). **Table 3-5** provides the data plan for configuring the SIP-based VoIP service.

Copyright © Huawei Technologies Co., Ltd.

In this example, the device runs in China. The default configurations of system parameters and the overseas feature parameters meet the standard and the application requirements. Therefore, you do not need to configure these parameters.

Table 3-5 provides the data plan for configuring the VoIP PSTN service (SIP).

Table 3-5 Data plan for configuring the VoIP PSTN service (SIP)

Item			Data
SIP interface data (The data configuration on the SIP interface must be the same as the data configuration on the IMS.)	Media and signaling parameters	Media and signaling upstream VLAN	Standard VLAN is recommended as the upstream VLAN of the VoIP service. Standard VLAN 20 is adopted.
		Media and signaling upstream port	In this office, all the services are transmitted upstream through the GIU board. Therefore, port 0/19/0 is used as the upstream port of the VoIP service.
		Media and signaling IP addresses	Next hop address from the MA5600T/MA5603T/MA5608T to the IMS core network device. **NOTICE** If the media IP address and the signaling IP address are different and the media and the signaling are transmitted upstream through different gateways, ensure that they correspond to correct gateways. Otherwise, normal calls may not be made.
	SIP interface (SIP) **NOTE** The parameters of the SIP interface must be the same as the parameters on the softswitch. SIP has many negotiation parameters, and the parameters here are mandatory.	The SIP interface ID	0 It is the SIP interface ID used for the VoIP service to be configured, which determines the virtual access gateway (VAG) specified for the user.
		Signaling port ID of the SIP interface	5060
		IP address of the primary softswitch to which the SIP interface belongs	IP address: 10.10.10.20/24 Port ID: 5060 When dual homing is configured, the IP address and the port ID of the secondary softswitch must also be configured.
		Port ID of the primary softswitch to which the SIP interface belongs	

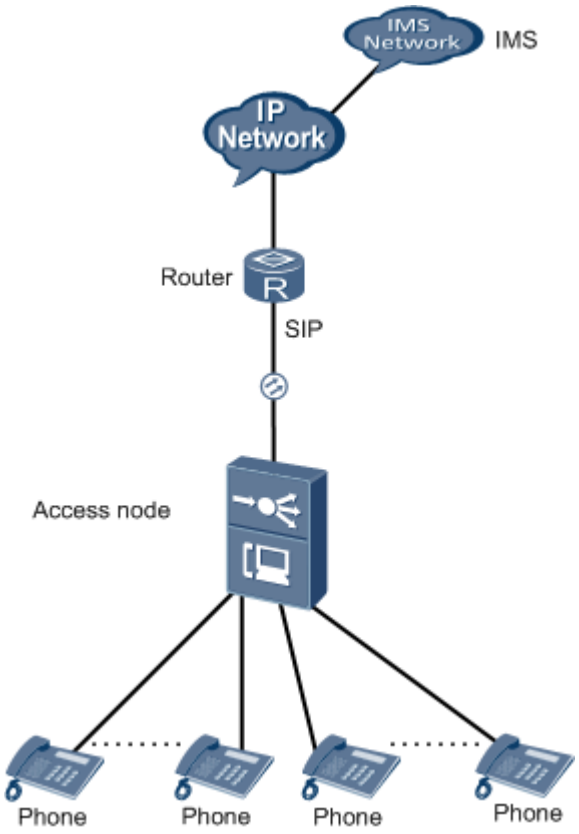
Copyright © Huawei Technologies Co., Ltd.

Item			Data
		Transmission mode of the SIP interface	UDP The transmission mode is selected according to the requirements on the softswitch. Generally, UDP is adopted.
		Home domain of the SIP interface	huawei
		Index of the profile used by the SIP interface (optional)	1
VoIP user data (The data configuration must be the same as the data configuration on the IMS.)	Slots that the boards reside in Voice service board (ASPB)		User access is implemented by the ASPB board in slot 0/2, 0/3.
	PSTN user data in slot 0/2	Numbers of Phone 0-Phone 63	83110000-83110063
		User priority	Phone 0: Cat2; Phone 1-Phone 63: Cat3 (default)
		User authentication	PSTN user whose port is 0/2/0, and telephone number is 83110000. ● Username: user83110000 ● Password: password mode, value: pwd83110000
	PSTN user data in slot 0/3	Numbers of Phone 64-Phone 127	88110000-88110063
		User type	Payphone
		PSTN port attributes	Polarity reversal pulse supported

Figure 3-11 shows an example network of the VoIP PSTN service (SIP).

Copyright © Huawei Technologies Co., Ltd.

Figure 3-11 Example network for configuring the VoIP PSTN service (SIP)



Prerequisite

- According to the actual network, a route from the MA5600T/MA5603T/MA5608T to the IMS must be configured to ensure that the MA5600T/MA5603T/MA5608T and the IMS are reachable from each other.
- Electronic switch 0 must be in **location-1** (indicating that the system goes upstream through only the upstream board). Electronic switch 1 must be in **location-0** (indicating that the VoIP service is supported). For details about how to configure the electronic switch, see **electro-switch**.

  NOTE

  - The SCUN and SCUH control boards do not support electronic switch.
  - The control board SCUL does not provide the upstream port and the system goes upstream through only the upstream board.

Procedure

Step 1 Add the upstream VLAN interface.

According to the data plan, configure standard VLAN 20 as the media and signaling upstream VLAN, add upstream port 0/19/0 to the VLAN, and configure the IP address of the Layer 3 interface to 10.10.10.10, which facilitates the configuration of the media and signaling IP address pools.

Copyright © Huawei Technologies Co., Ltd.

```
huawei(config)#vlan 20 standard
huawei(config)#port vlan 20 0/19 0
huawei(config)#interface vlanif 20
huawei(config-if-vlanif20)#ip address 10.10.10.10 24
huawei(config-if-vlanif20)#quit
```

Step 2 Configure the media and signaling IP address pools.

Add the IP address of the VLAN Layer 3 interface configured in the previous step to the media and signaling IP address pools respectively, which facilitates the selection of media and signaling IP addresses used for the services from the IP address pools. According to the data plan, IP address 10.10.10.10 is added to the media and signaling IP address pools, and the gateway IP address corresponding to the media IP address is 10.10.10.1.

```
huawei(config)#voip
huawei(config-voip)#ip address media 10.10.10.10 10.10.10.1
huawei(config-voip)#ip address signaling 10.10.10.10
huawei(config-voip)#quit
```

NOTE

- You can configure the attributes of the H248 or MG interface only when the media IP address and the signaling IP address exist in the media and signaling IP address pools.
- The media IP address and the signaling IP address can be different. You can plan the IP addresses according to the actual network.

Step 3 Add an SIP interface.

Add an SIP interface to communicate with the IMS, which ensures that the IMS can control the call connection through the SIP interface. According to the data plan, add SIP interface 0, and configure the interface attributes.

- Signaling/Media IP address: 10.10.10.10
- Signaling port ID: 5060
- Transfer mode: UDP
- IP address of the primary IMS: 10.10.10.20
- Signaling port ID of the primary IMS: 5060
- Homing domain name of SIP interface: huawei
- SIP profile ID: 1

```
huawei(config)#interface sip 0
  Are you sure to add SIP interface?(y/n)[n]:y
huawei(config-if-sip-0)#if-sip attribute basic media-ip 10.10.10.10
 signal-ip 10.10.10.10 signal-port 5060 transfer udp primary-proxy-ip1 10.10.10.20
primary-proxy-port
5060 home-domain huawei sipprofile-index 1
```

Step 4 Configure the ringing mapping of SIP interface 0.

Configure the user ringing mode. The break-make ratios of the cadence ringing and the initial ringing are both 1:4. Therefore, the value of parameter *cadence* is 0, and the value of parameter *initialring* is 4.

```
huawei(config-if-sip-0)#ringmode add 0 ringname cadencering 0 initialring 4
```

Step 5 Enable the SIP interface.

Reset the SIP interface to make the SIP interface register with the IMS (or to make the attributes of the SIP interface take effect), so that the SIP interface can work in the normal state.

Copyright © Huawei Technologies Co., Ltd.

```
huawei(config-if-sip-0)#reset
  Are you sure to reset the SIP interface?(y/n)[n]:y
huawei(config-if-sip-0)#quit
```

Step 6 Query the running status of the SIP interface.

After the SIP interface is interconnected with the IMS, the SIP interface should be in the normal state, indicating that the SIP interface can work in the normal state.

```
huawei>display if-sip all
------------------------------------------------------------
  MGID                                0
  Transfer Mode                       UDP
  State                               Normal
  Signalling IP                       192.168.0.170
  Signalling Port                     5068
  Primary Proxy IP 1/DomainName       192.168.0.171
  Primary Proxy Port                  5060
  Primary Proxy State                 Up
  Secondary Proxy IP 1/DomainName     192.168.0.172
  Secondary Proxy Port                5061
  Secondary Proxy State               Up
  Current Proxy                       Primary Proxy
------------------------------------------------------------
```

Step 7 Configure the PSTN subscriber data.

1. Configure the PSTN user data (Phone 0-Phone 63) in slot 0/2.

   ```
   huawei(config)#esl user
   huawei(config-esl-user)#sippstnuser batadd 0/2/0 0/2/63 0 telno 83110000
   ```

2. Configure the calling priority of the PSTN user in port 0/2/0 as Cat2.

   ```
   huawei(config-esl-user)#sippstnuser attribute set 0/2/0 priority cat2
   ```

3. Configure the PSTN user data (Phone 64-Phone 127) in slot 0/3.

   ```
   huawei(config-esl-user)#sippstnuser batadd 0/3/0 0/3/63 0 telno 88110000
   ```

4. Configure the authentication data of the PSTN user in port 0/2/0.

   ```
   huawei(config-esl-user)#sippstnuser auth set 0/2/0 telno 83110000 password-
   mode password
     User Name(<=64 characters, "-" indicates deletion):user83110000
     User Password(<=64 characters, "-" indicates deletion):    //Input the
   password pwd8311000
   ```

   NOTE

   Considering users safety, the IMS may require user authentication. You can run the **sippstnuser auth set** command to configure the user authentication data, including user name, password mode and password. The authentication data should be consistent with that of IMS side.

5. Configure the PSTN user type in slot 0/3.

   ```
   huawei(config-esl-user)#sippstnuser attribute batset 0/3/0 0/3/63 potslinetype
   PayPhone
   huawei(config-esl-user)#quit
   ```

Step 8 Configure the PSTN port attributes.

Configure the PSTN port in slot 0/3 so that the port supports the polarity reversal.

```
huawei(config)#pstnport
huawei(config-pstnport)#pstnport attribute batset 0/3/0 0/3/63 reverse-pole-pulse
enable
huawei(config-pstnport)#quit
```

Step 9 Save the data.

Copyright © Huawei Technologies Co., Ltd.

```
huawei(config)#save
```

----End

Result

After the interface data and the PSTN user data corresponding to the SIP interface are configured on the IMS, check whether the VoIP services can be provisioned normally. In the normal state, users of Phone 0-Phone 127 can communicate with each other successfully.

- The calling party can hear the dialing tone after picking up the phone.
- When the calling party dials the phone number of the called party, the phone of the called party can ring normally, and the calling party can hear the ring-back tone.
- The calling party and the called party can communicate in the normal state.
- After the called party hooks on, the calling party can hear the busy tone.

Configuration File

The following describes the configuration file of this configuration example. Note that certain steps must be performed manually and the configuration file cannot be imported directly.

Configure the upstream VLAN interface.

```
vlan 20 standard
port vlan 20 0/19 0
interface vlanif 20
ip address 10.10.10.10 24
quit
```

Configure the media and signaling IP address pools.

```
voip
ip address media 10.10.10.10 10.10.10.1
ip address signaling 10.10.10.10
```

Add an SIP interface and configure the attributes of the SIP interface.

```
if-sip attribute basic media-ip 10.10.10.10
 signal-ip 10.10.10.10 signal-port 5060 transfer udp primary-proxy-ip1 10.10.10.20
 primary-proxy-port 5060 home-domain huawei sipprofile-index 1
```

Configure the ringing mapping of the SIP interface.

```
ringmode add 0 ringname cadencering 0 initialring 4
```

Enable the SIP interface.

```
reset
quit
```

Query the running status of the SIP interface.

```
display if-sip all
```

Confirm the service board.

```
board confirm 0/2
board confirm 0/3
```

Configure the PSTN user data.

```
esl user
sippstnuser batadd 0/2/00/2/63 0 telno 83110000
```


Copyright © Huawei Technologies Co., Ltd.

```
sippstnuser attribute set 0/2/0 priority cat2
sippstnuser auth set 0/2/0 telno 83110000 password-mode password
sippstnuser batadd 0/3/0 0/3/63 0 telno 88110000
sippstnuser attribute batset 0/3/0 0/3/63 potslinetype PayPhone
quit
```

Configure the polarity reversal accounting function.

```
pstnport
pstnport attribute batset 0/3/0 0/3/63 reverse-pole-pulse enable
quit
```

Save the data.

```
save
```

3.3.4 Example: Configuring the VoIP Service (H.248-based and SIP-based)

This topic describes an example for configuring the H.248-based and SIP-based VoIP service. The MA5600T/MA5603T/MA5608T supports the H.248-based VoIP service and the SIP-based VoIP service at the same time.

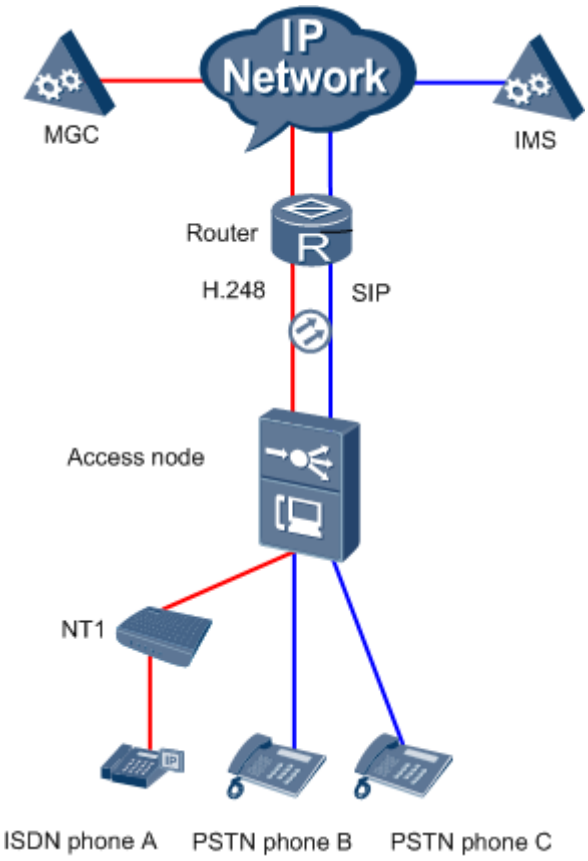
Service Requirements

- The MA5600T/MA5603T/MA5608T upstream to NGN network for ISDN service by adopting the H.248 protocol. The MA5600T/MA5603T/MA5608T upstream to IMS network for PSTN service by adopting the SIP protocol.
- ISDN Phone A is connected to the MA5600T/MA5603T/MA5608T through the NT1, and the ISDN digital phone supports the P2P function.
- Basic rate interface (BRI) is adopted between the NT1 and the MA5600T/MA5603T/MA5608T to provide a rate of 144 kbit/s, including two B channels and one D channel.
- The Phone B and Phone C are PSTN users, the user priority is **Cat2**.
- After the configuration is completed, normal calls can be made between two phone sets.

Figure 3-12 shows an example network of the VoIP service that based the SIP protocol and H.248 protocol.

Copyright © Huawei Technologies Co., Ltd.

Figure 3-12 the network of the VoIP service that based the SIP protocol and H.248 protocol.



Prerequisite

- The MA5600T/MA5603T must use the H.248 protocol to communicate with the MGC and use the SIP protocol to communicate with the IMS.
- The H.248 interface and the system parameters must be configured. For the related operations, see Configuring an MG Interface and (Optional) Configuring the System Parameters. The H.248 interface must be in the normal state.
- The SIP interface and the system parameters must be configured. For the related operations, see Configuring an SIP Interface and (Optional) Configuring the System Parameters. The SIP interface must be in the normal state.
- The system must be configured with the ISDN service board, that is, the DSRD board or DSRE board.
- The system must be configured with the PSTN service board, that is, the ASRB board or ASPB board.
- The ISDN digital phone must support the P2P function.
- The terminal endpoint identifier of the ISDN digital phone must be 0.

Data Plan

Table 3-6 provides the data plan .

Copyright © Huawei Technologies Co., Ltd.

Table 3-6 Data plan

Item		Data
The data plan of the ISDN BRA service based H.248 protocol		
H.248 interface ID		0
IUA link set parameter	IUA link set ID	1
	Working mode of a link set	override
	Pending time	10s
	Mode of generating the interface ID	2
	Whether the link in the link set supports the interlocking	enable
	Service environment corresponding to the IUA link set	client
IUA link parameter	IUA link ID	15
	Local port ID	1401
	Local IP address	10.13.4.116/16 (It must exist in the signaling IP address pool.)
	Remote port ID	1400
	IP address of the primary MGC	10.14.1.2/16 (IP address of the primary MGC)
	MGC that is bound to the IUA link	primary-mgc
	Priority of the IUA link.	3
ISDN BRA port	Subrack ID/ Slot ID/Port ID	0/2/0
	IUA interface ID	8
	Working mode	P2P

Copyright © Huawei Technologies Co., Ltd.

Item		Data
	TID	100, 110
	Phone number	12345601, 12345602
	Automatic deactivation	Disabled
	Activation mode	Stable activation
The data plan of the PSTN service based SIP protocol		
SIP interface ID		0
PSTN port (The data configuration must be the same as the data configuration on the IMS.)	Frame/slot/port	0/3/0, 0/3/1.
	Numbers of Phone	83110000, 83110001
	User priority	Cat2
	User type	Payphone
	PSTN port attributes	Polarity reversal pulse supported

Procedure

- Configure the H.248-based ISDN service
  1. Configure the working mode of the ISDN BRA port.

     In the BRA port mode, configure the working mode of the ISDN BRA port to P2P, configure the activation mode to stable activation, and disable automatic activation.

     ```
     huawei(config)#braport
     huawei(config-braport)#braport attribute set 0/2/0 workmode p2p
     activemode stable-active autodeactive disable
     huawei(config-braport)#quit
     ```

  2. Add an IUA link set and IUA links.

     In the SIGTRAN mode, configure the SIGTRAN protocol stack. Add an IUA link set, and then add IUA links.

     ```
     huawei(config)#sigtran
     huawei(config-sigtran)#iua-linkset add 1 mgid 0 jointly-work enable
     trafficmode override
     iid-map 2 pendingtime 1 cs-mode client
     huawei(config-sigtran)#iua-link add 15 1 1401 10.13.4.116 1400 10.14.1.2
     jointly-work-with primary-mgc priority 3
     huawei(config-sigtran)#quit
     ```

     NOTE

     All the ISDN call control messages are sent from the IUA link to the softswitch, whereas the system uses the bearer control messages to communicate with the softswitch through H.248.

  3. Configure the ISDN BRA user data.

     ```
     huawei(config)#esl user
     huawei(config-esl-user)#mgbrauser add 0/2/0 0 1 interfaceid 8 terminalid
     ```


Copyright © Huawei Technologies Co., Ltd.

```
100 telno 12345601
huawei(config-esl-user)#quit
```

NOTICE

Each ISDN BRA user occupies two TIDs. You need to input only the first TID when adding an ISDN BRA user.

- When the TID profile to which the ISDN BRA user of the MG interface is bound is not a layering profile, the TID must be configured and must differ from the TID of the existing ISDN BRA user by an integer multiple of 2.
- When the TID profile to which the ISDN BRA user of the MG interface is bound is a layering profile, the configuration of the TID is optional because the system automatically allocates the TID.

- Configure the SIP-based PSTN service
  1. Add the ASPB service board.

     According to the data plan, add a ASPB board to slot0/3.

     ```
     huawei(config)#board add 0/3 ASP
     huawei(config)#board confirm 0/3
     ```

  2. Configure the PSTN subscriber data.

     According to the data plan, configure a telephone number and priority of the PSTN user.

     ```
     huawei(config)#esl user
     huawei(config-esl-user)#sippstnuser batadd 0/3/0 0/3/1 0 telno 83110000
     huawei(config-esl-user)#sippstnuser attribute set 0/3/0 priority cat2
     huawei(config-esl-user)#sippstnuser attribute set 0/3/1 priority cat2
     huawei(config-esl-user)#quit
     ```

  3. Configure the PSTN port attributes.

     ```
     huawei(config)#pstnport
     huawei(config-pstnport)#pstnport attribute batset 0/3/0 0/3/1 reverse-
     pole-pulse enable
     huawei(config-pstnport)#quit
     ```

  4. Save the data.

     ```
     huawei(config)#save
     ```

----End

Result

After the configuration is completed, users of ports 0/2/0, 0/3/0, and 0/3/1 can call each other successfully.

Configuration File

```
board add 0/2 H802DSRD
board confirm 0/2
braport
braport attribute set 0/2/0 workmode p2p activemode stable-active autodeactive
disable
quit
sigtran
iua-linkset add 1 mgid 0 jointly-work enable trafficmode override
```


Copyright © Huawei Technologies Co., Ltd.

```
iid-map 2 pendingtime 1 cs-mode client
iua-link add 15 1 1401 10.13.4.116 1400 10.14.1.2
jointly-work-with primary-mgc priority 3
quit
esl user
mgbrauser add 0/2/0 0 1 interfaceid 8 terminalid 100 telno 12345601
quit
board add 0/3 ASP
board confirm 0/3
esl user
sippstnuser batadd 0/3/00/3/1 0 telno 83110000
sippstnuser attribute set 0/3/0 priority cat2
sippstnuser attribute set 0/3/1 priority cat2
quit
pstnport
pstnport attribute batset 0/3/0 0/3/1 reverse-pole-pulse enable
quit
save
```

3.3.5 Example: Configuring the P2P ISDN BRA Service

This topic describes how to configure the P2P ISDN BRA service on the MA5600T/MA5603T/MA5608T, which is applicable to the scenario where one NT1 is connected to only one terminal.

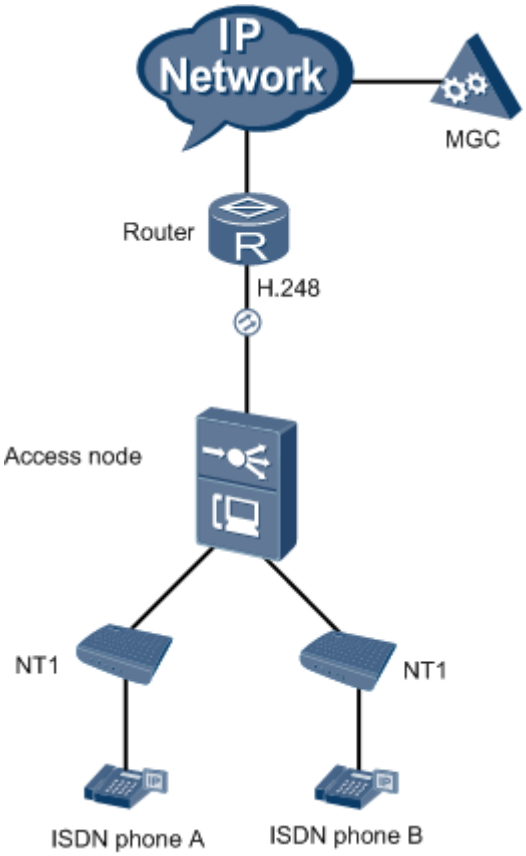
Service Requirements

- ISDN Phone A is connected to the MA5600T/MA5603T/MA5608T through the NT1, and the ISDN digital phone supports the P2P function.
- ISDN Phone B is connected to the MA5600T/MA5603T/MA5608T through the NT1, and the ISDN digital phone supports the P2P function.
- Basic rate interface (BRI) is adopted between the NT1 and the MA5600T/MA5603T/MA5608T to provide a rate of 144 kbit/s, including two B channels and one D channel.
- After the configuration is completed, normal calls can be made between two phone sets.

Figure 3-13 shows an example network of the P2P ISDN BRA service.

Copyright © Huawei Technologies Co., Ltd.

Figure 3-13 Example network of the P2P ISDN BRA service



Prerequisite

- The MG interface and the system parameters must be configured. For the related operations, see Configuring an MG Interface and (Optional) Configuring the System Parameters. The MG interface must be in the normal state.
- The ISDN digital phone must support the P2P function.
- The system must be configured with the ISDN service board, that is, the DSRD or DSRE board.
- The terminal endpoint identifier of the ISDN digital phone must be 0.

Data Plan

Table 3-7 provides the data plan for configuring the P2P ISDN BRA service.

Table 3-7 Data plan for configuring the P2P ISDN BRA service

Item		Data
MG interface ID		0
IUA link set parameter	IUA link set ID	1

Copyright © Huawei Technologies Co., Ltd.

Item		Data
	Working mode of a link set	override
	Pending time	10s
	Mode of generating the interface ID	2
	Whether the link in the link set supports the interlocking	enable
	Service environment corresponding to the IUA link set	client
IUA link parameter	IUA link ID	15
	Local port ID	1401
	Local IP address	10.13.4.116/16 (It must exist in the signaling IP address pool.)
	Remote port ID	1400
	IP address of the primary MGC	10.14.1.2/16 (IP address of the primary MGC)
	MGC that is bound to the IUA link	primary-mgc
	Priority of the IUA link.	3
	IP address of the primary MGC	10.14.1.2/16 (IP address of the primary MGC)
ISDN BRA port	Subrack ID/ Slot ID/Port ID	0/2/0, 0/3/0
	IUA interface ID	8, 9
	Working mode	P2P
	TID	100, 110

Copyright © Huawei Technologies Co., Ltd.

Item		Data
	Phone number	12345601, 12345602
	Automatic deactivation	Disabled
	Activation mode	Stable activation

Procedure

Step 1 Configure the working mode of the ISDN BRA port.

In the BRA port mode, configure the working mode of the ISDN BRA port to P2P, configure the activation mode to stable activation, and disable automatic activation.

```
huawei(config)#braport
huawei(config-braport)#braport attribute set 0/2/0 workmode p2p activemode stable-active autodeactive disable
huawei(config-braport)#braport attribute set 0/3/0 workmode p2p activemode stable-active autodeactive disable
huawei(config-braport)#quit
```

Step 2 Add an IUA link set and IUA links.

In the SIGTRAN mode, configure the SIGTRAN protocol stack. Add an IUA link set, and then add IUA links.

```
huawei(config)#sigtran
huawei(config-sigtran)#iua-linkset add 1 mgid 0 jointly-work enable trafficmode override
iid-map 2 pendingtime cs-mode client
huawei(config-sigtran)#iua-link add 15 1 1401 10.13.4.116 1400 10.14.1.2 jointly-work-with primary-mgc priority 3
huawei(config-sigtran)#quit
```

NOTE

All the ISDN call control messages are sent from the IUA link to the softswitch, whereas the system uses the bearer control messages to communicate with the softswitch through H.248.

Step 3 Configure the ISDN BRA user data.

```
huawei(config)#esl user
huawei(config-esl-user)#mgbrauser add 0/2/0 0 1 interfaceid 8 terminalid 100 telno 12345601
huawei(config-esl-user)#mgbrauser add 0/3/0 0 1 interfaceid 9 terminalid 110 telno 12345602
huawei(config-esl-user)#quit
```


Copyright © Huawei Technologies Co., Ltd.

NOTICE

Each ISDN BRA user occupies two TIDs. You need to input only the first TID when adding an ISDN BRA user.

- When the TID profile to which the ISDN BRA user of the MG interface is bound is not a layering profile, the TID must be configured and must differ from the TID of the existing ISDN BRA user by an integer multiple of 2.
- When the TID profile to which the ISDN BRA user of the MG interface is bound is a layering profile, the configuration of the TID is optional because the system automatically allocates the TID.

Step 4 Save the data.

```
huawei(config)#save
```

----End

Result

After the configuration is completed, two ISDN BRA users of ports 0/2/0 and 0/3/0 can call each other successfully.

Configuration File

```
board add 0/2 H802DSRD
board add 0/3 H802DSRD
board confirm 0/2
board confirm 0/3
braport
braport attribute set 0/2/0 workmode p2p activemode stable-active autodeactive
disable
braport attribute set 0/3/0 workmode p2p activemode stable-active autodeactive
disable
quit
sigtran
iua-linkset add 1 mgid 0 jointly-work enable trafficmode override
iid-map 2 pendingtime cs-mode client
iua-link add 15 1 1401 10.13.4.116 1400 10.14.1.2
jointly-work-with primary-mgc priority 3quit
esl user
mgbrauser add 0/2/0 0 1 interfaceid 8 terminalid 100 telno 12345601
mgbrauser add 0/3/0 0 1 interfaceid 9 terminalid 110 telno 12345602
quit
save
```

3.3.6 Example: Configuring the P2P ISDN BRA Service (Based on the SIP Protocol)

This topic describes how to configure the P2P ISDN BRA service on the MA5600T/MA5603T/MA5608T, which is applicable to the scenario where one NT1 is connected to only one terminal.

Service Requirements

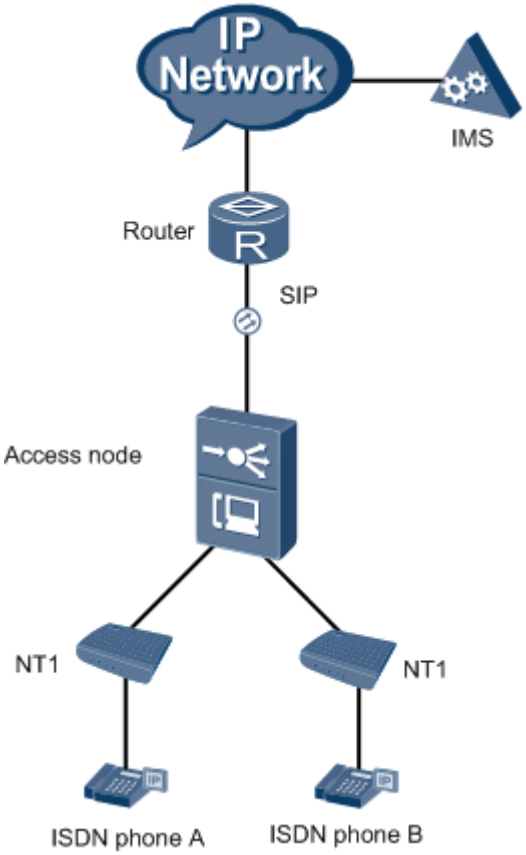
- ISDN Phone A is connected to the MA5600T/MA5603T/MA5608T through the NT1, and the ISDN digital phone supports the P2P function.

Copyright © Huawei Technologies Co., Ltd.

- ISDN Phone B is connected to the MA5600T/MA5603T/MA5608T through the NT1, and the ISDN digital phone supports the P2P function.
- Basic rate interface (BRI) is adopted between the NT1 and the MA5600T/MA5603T/MA5608T to provide a rate of 144 kbit/s, including two B channels and one D channel.
- After the configuration is completed, normal calls can be made between two phone sets.

Figure 3-14 shows an example network of the P2P ISDN BRA service.

Figure 3-14 Example network of the P2P ISDN BRA service



Prerequisite

- The MA5600T/MA5603T/MA5608T must use the SIP protocol to communicate with the IMS.
- The MG interface and the system parameters must be configured. For the related operations, see Configuring an SIP Interface and (Optional) Configuring the System Parameters. The MG interface must be in the normal state.
- The ISDN digital phone must support the P2P function.
- The system must be configured with the ISDN service board, that is, the DSRD board or the DSRE board .
- The terminal endpoint identifier of the ISDN digital phone must be 0.

Copyright © Huawei Technologies Co., Ltd.

Data Plan

Table 3-8 provides the data plan for configuring the P2P ISDN BRA service.

Table 3-8 Data plan for configuring the P2P ISDN BRA service

Item		Data
MG interface ID		0
ISDN BRA port	Subrack ID/ Slot ID/Port ID	0/2/0, 0/3/0
	Working mode	P2P
	Phone number	12345601, 12345602
	Automatic deactivation	Disabled
	Activation mode	Stable activation

Procedure

Step 1 Configure the working mode of the ISDN BRA port.

In the BRA port mode, configure the working mode of the ISDN BRA port to P2P, configure the activation mode to stable activation, and disable automatic activation.

```
huawei(config)#braport
huawei(config-braport)#braport attribute set 0/2/0 workmode p2p activemode stable-active autodeactive disable
huawei(config-braport)#braport attribute set 0/3/0 workmode p2p activemode stable-active autodeactive disable
huawei(config-braport)#quit
```

Step 2 Configure the ISDN BRA user data.

```
huawei(config)#esl user
huawei(config-esl-user)#sipbrauser add 0/2/0 0 telno 12345601
huawei(config-esl-user)#sipbrauser add 0/3/0 0 telno 12345602
huawei(config-esl-user)#quit
```

Step 3 Save the data.

```
huawei(config)#save
```

----End

Result

After the configuration is completed, two ISDN BRA users of ports 0/2/0 and 0/3/0 can call each other successfully.

Configuration File

```
braport
braport attribute set 0/2/0 workmode p2p activemode stable-active autodeactive
```


Copyright © Huawei Technologies Co., Ltd.

```
disable
braport attribute set 0/3/0 workmode p2p activemode stable-active autodeactive
disable
quit
esl user
sipbrauser add 0/2/0 0 telno 12345601
sipbrauser add 0/3/0 0 telno 12345602
quit
save
```

3.3.7 Example: Configuring the P2MP ISDN BRA Service

This topic describes how to configure the P2MP ISDN BRA service on the MA5600T/MA5603T/MA5608T, which is applicable to the scenario where one NT1 is connected to multiple terminals.

Service Requirements

- Two ISDN digital phones are connected to the MA5600T/MA5603T/MA5608T through the same NT1.
- Basic rate interface (BRI) is adopted between the NT1 and the MA5600T/MA5603T/MA5608T to provide a rate of 144 kbit/s, including two B channels and one D channel.

Prerequisite

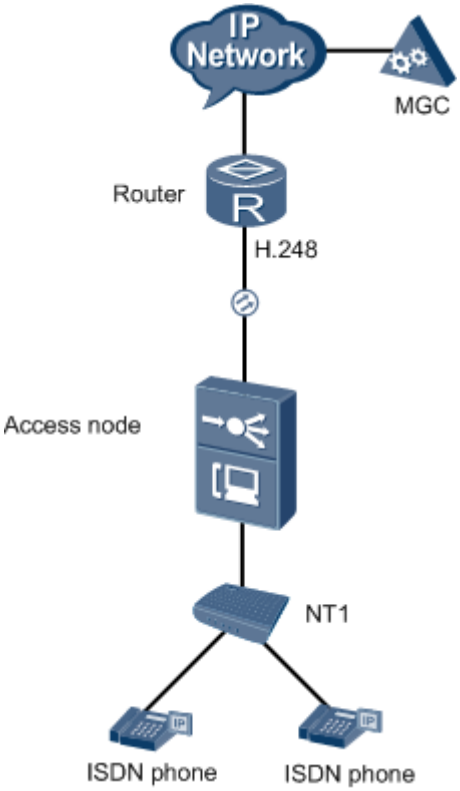
- The MG interface and the system parameters must be configured. For the related operations, see Configuring an MG Interface and (Optional) Configuring the System Parameters. The MG interface must be in the normal state.

Networking

Figure 3-15 shows an example network of the P2MP ISDN BRA service.

Copyright © Huawei Technologies Co., Ltd.

Figure 3-15 Example network of the P2MP ISDN BRA service



Data Plan

Table 3-9 provides the data plan for configuring the P2MP ISDN BRA service.

Table 3-9 Data plan for the P2MP ISDN BRA service

Item		Data
MG interface ID		0
IUA link set parameter	IUA link set ID	1
	Working mode of a link set	override
	Pending time	10s
	Mode of generating the interface ID	2
	Whether the link in the link set supports the interlocking	enable

Copyright © Huawei Technologies Co., Ltd.

Item		Data
	Service environment corresponding to the IUA link set	client
IUA link parameter	IUA link ID	15
	Local port ID	1401
	Local IP address	10.13.4.116/16 (It must exist in the signaling IP address pool.)
	Remote port ID	1400
	IP address of the primary MGC	10.14.1.2/16 (IP address of the primary MGC)
	MGC that is bound to the IUA link	primary-mgc
	Priority of the IUA link.	3
	IP address of the primary MGC	10.14.1.2/16 (IP address of the primary MGC)
ISDN BRA port	Subrack ID/Slot ID/Port ID	0/3/1
	IUA interface ID	10
	Working mode	P2MP
	TID	106
	Phone number	88880000

Procedure

Step 1 Configure the working mode of the ISDN BRA port.

In the BRA port mode, configure the working mode of the ISDN BRA port to P2MP, configure the activation mode to stable activation, and enable automatic activation.

```
huawei(config)#braport
huawei(config-braport)#braport attribute set 0/3/1 workmode p2mp autodeactive enable
```

Step 2 Add an IUA link set and IUA links.

In the SIGTRAN mode, configure the SIGTRAN protocol stack. Add an IUA link set, and then add IUA links.

```
huawei(config-braport)#quit
huawei(config)#sigtran
huawei(config-sigtran)#iua-linkset add 1 mgid 0 jointly-work enable trafficmode override
```


Copyright © Huawei Technologies Co., Ltd.

```
iid-map 2 pendingtime cs-mode client
huawei(config-sigtran)#iua-link add 15 1 1401 10.13.4.116 1400 10.14.1.2
jointly-work-with primary-mgc priority 3
```

Step 3 Configure the ISDN BRA user data.

```
huawei(config-sigtran)#quit
huawei(config)#esl user
huawei(config-esl-user)#mgbrauser add 0/3/1 0 1 interfaceid 10 terminalid 106
telno 88880000
```

Step 4 Save the data.

```
huawei(config-esl-user)#quit
huawei(config)#save
```

----End

Result

After the configuration is completed, two ISDN BRA users of the NT1 connected to port 0/3/1 can make calls successfully.

Configuration File

```
braport
braport attribute set 0/3/1 workmode p2mp autodeactive enable
quit
sigtran
iua-linkset add 1 mgid 0 jointly-work enable trafficmode override
iid-map 2 pendingtime cs-mode client
iua-link add 15 1 1401 10.13.4.116 1400 10.14.1.2
jointly-work-with primary-mgc priority 3
quit
esl user
mgbrauser add 0/3/1 0 1 interfaceid 10 terminalid 106  telno 88880000
quit
save
```

3.3.8 Example: Configuring the P2MP ISDN BRA Service(Based on the SIP Protocol)

This topic describes how to configure the P2MP ISDN BRA service on the MA5600T/MA5603T/MA5608T, which is applicable to the scenario where one NT1 is connected to multiple terminals.

Service Requirements

- Two ISDN digital phones are connected to the MA5600T/MA5603T/MA5608T through the same NT1.
- Basic rate interface (BRI) is adopted between the NT1 and the MA5600T/MA5603T/MA5608T to provide a rate of 144 kbit/s, including two B channels and one D channel.
- Normal calls can be made on both phones.

Prerequisite

- The MA5600T/MA5603T/MA5608T must use the SIP protocol to communicate with the IMS.

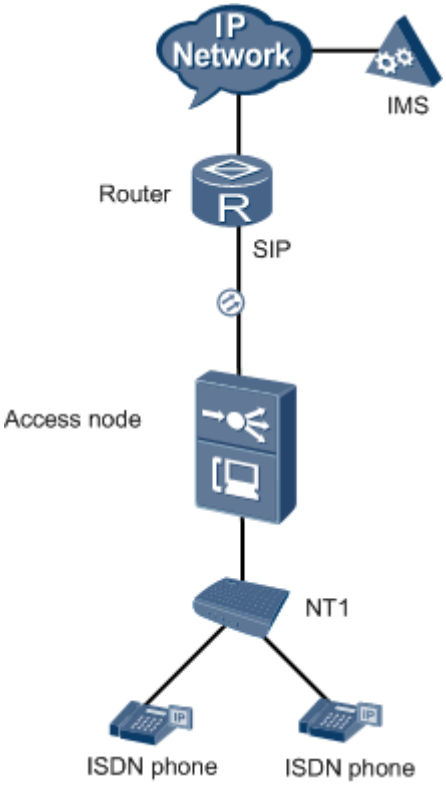
Copyright © Huawei Technologies Co., Ltd.

- The MG interface and the system parameters must be configured. For the related operations, see Configuring an SIP Interface and (Optional) Configuring the System Parameters. The MG interface must be in the normal state.
- The system must be configured with the ISDN service board, that is, the DSRD board or the DSRE board .

Networking

Figure 3-16 shows an example network of the P2MP ISDN BRA service.

Figure 3-16 Example network of the P2MP ISDN BRA service



Data Plan

Table 3-10 provides the data plan for configuring the P2MP ISDN BRA service.

Table 3-10 Data plan for the P2MP ISDN BRA service

Item		Data
MG interface ID		0
ISDN BRA port	Subrack ID/Slot ID/Port ID	0/3/1
	Working mode	P2MP

Copyright © Huawei Technologies Co., Ltd.

Item		Data
	Phone number	88880000

Procedure

Step 1 Configure the working mode of the ISDN BRA port.

In the BRA port mode, configure the working mode of the ISDN BRA port to P2MP, configure the activation mode to stable activation, and enable automatic activation.

```
huawei(config)#braport
huawei(config-braport)#braport attribute set 0/3/1 workmode p2mp autodeactive enable
huawei(config-braport)#quit
```

Step 2 Configure the ISDN BRA user data.

```
huawei(config)#esl user
huawei(config-esl-user)#sipbrauser add 0/3/1 0 telno 88880000
huawei(config-esl-user)#quit
```

Step 3 Save the data.

```
huawei(config)#save
```

----End

Result

After the configuration is completed, two ISDN BRA users of the NT1 connected to port 0/3/1 can make calls successfully.

Configuration File

```
braport
braport attribute set 0/3/1 workmode p2mp autodeactive enable
quit
esl user
sipbrauser add 0/3/1 0 telno 88880000
quit
save
```

3.3.9 Example: Configuring the ISDN PRA Service

This topic is applicable to the scenario where the ISDN users are connected to the MA5600T/MA5603T/MA5608T through the ISDN primary rate interface (PRI).

Prerequisite

- The PSTN user (Phone B in the example network) must be configured and can communicate with other users in the normal state. For the configuration method, see **3.3.1 Example: Configuring the VoIP Service (H.248-based)**.
- Users of the PBX must be configured and can communicate with each other in the normal state.
- The system must be configured with the EDTB board.

Copyright © Huawei Technologies Co., Ltd.

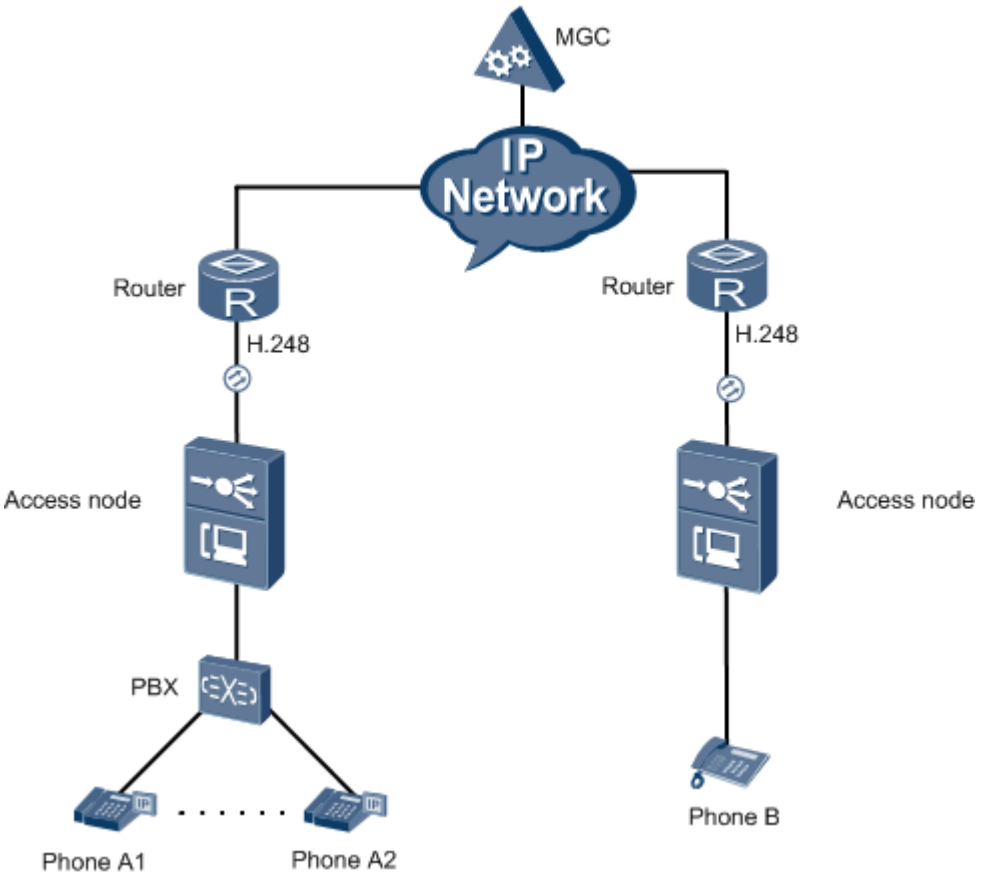
Service Requirements

- The PBX is connected to the MA5600T/MA5603T/MA5608T through the ISDN PRI. PRI supports a data rate of 2048 kbit/s, including 30 B channels and one D channel. The rate of both the B channel and the D channel is 64 kbit/s.
- After the configuration is completed, users of the PBX can make calls successfully and can communicate with users outside the PBX in the normal state.

Networking

Figure 3-17 shows an example of the ISDN PRA service.

Figure 3-17 Example of the ISDN PRA service



Data Plan

Table 3-11 provides the data plan for configuring the ISDN PRA service.

Table 3-11 Data plan for configuring the ISDN PRA service

Item	Data
MG interface ID	0

Copyright © Huawei Technologies Co., Ltd.

Item		Data
IUA link set parameter	IUA link set ID	1
	Working mode of a link set	override
	Pending time	10s
	Mode of generating the interface ID	2
	Whether the link in the link set supports the interlocking	enable
	Service environment corresponding to the IUA link set	client
IUA link parameter	IUA link ID	15
	Local port ID	1401
	Local IP address	10.13.4.116/16 (It must exist in the signaling IP address pool.)
	Remote port ID	1400
	IP address of the primary MGC	10.14.1.2/16 (IP address of the primary MGC)
	MGC that is bound to the IUA link	primary-mgc
	Priority of the IUA link.	3
	IP address of the primary MGC	10.14.1.2/16 (IP address of the primary MGC)
ISDN PRA port	Subrack ID/Slot ID/Port ID	0/2/0
	IUA interface ID	1
	TID	512

Procedure

Step 1 Add the EDTB board.

According to the data plan, add an ISDN PRA service board to slot 0/2.

Copyright © Huawei Technologies Co., Ltd.

```
huawei(config)#board add 0/2 h802EDTB
```

Step 2 Add an IUA link set and IUA links.

In the SIGTRAN mode, configure the SIGTRAN protocol stack. Add an IUA link set, and then add IUA links.

```
huawei(config)#sigtran
huawei(config-sigtran)#iua-linkset add 1 mgid 0 jointly-work enable trafficmode
override
iid-map 2 pendingtime cs-mode client
huawei(config-sigtran)#iua-link add 15 1 1401 10.13.4.116 1400 10.14.1.2
jointly-work-with primary-mgc priority 3
```

NOTE

All the ISDN call control messages are sent from the IUA link to the softswitch, whereas the system uses the bearer control messages to communicate with the softswitch through H.248.

Step 3 Configure the ISDN PRA user data.

```
huawei(config-sigtran)#quit
huawei(config)#esl user
huawei(config-esl-user)#mgprauser add 0/2/0 0 1 interfaceid 1 terminalid 512
```

NOTICE

Each ISDN PRA user occupies 32 TIDs. You need to input only the first TID when adding an ISDN PRA user.

- When the TID profile to which the ISDN PRA user of the MG interface is bound is not a layering profile, the TID must be configured and cannot be within the configured TID range.
- When the TID profile to which the ISDN PRA user of the MG interface is bound is a layering profile, the configuration of the TID parameter is not available because the system automatically allocates the TID.

Step 4 Save the data.

```
huawei(config-esl-user)#quit
huawei(config)#save
```

----End

Result

After the configuration is completed, all the users of the PBX can communicate with Phone B in the normal state.

Configuration File

```
board add 0/2 h802EDTB
sigtran
iua-linkset add 1 mgid 0 jointly-work enable trafficmode override
iid-map 2 pendingtime cs-mode client
iua-link add 15 1 1401 10.13.4.116 1400 10.14.1.2
jointly-work-with primary-mgc priority 3
quit
esl user
mgprauser add 0/2/0 0 1 interfaceid 1 terminalid 512
quit
save
```


Copyright © Huawei Technologies Co., Ltd.

3.3.10 Example: Configuring the ISDN PRA Service (Based on the SIP Protocol)

This topic is applicable to the scenario where the ISDN users are connected to the MA5600T/MA5603T/MA5608T through the ISDN primary rate interface (PRI).

Prerequisite

- The MA5600T/MA5603T/MA5608T must use the SIP protocol to communicate with the IMS.
- The MG interface and the system parameters must be configured. For the related operations, see Configuring an SIP Interface and (Optional) Configuring the System Parameters. The MG interface must be in the normal state.
- The PSTN user (Phone B in the example network) must be configured and can communicate with other users in the normal state. For the configuration method, see **3.3.3 Example: Configuring the VoIP PSTN Service (SIP)**.
- Users of the PBX must be configured and can communicate with each other in the normal state.
- The system must be configured with the EDTB board.

Service Requirements

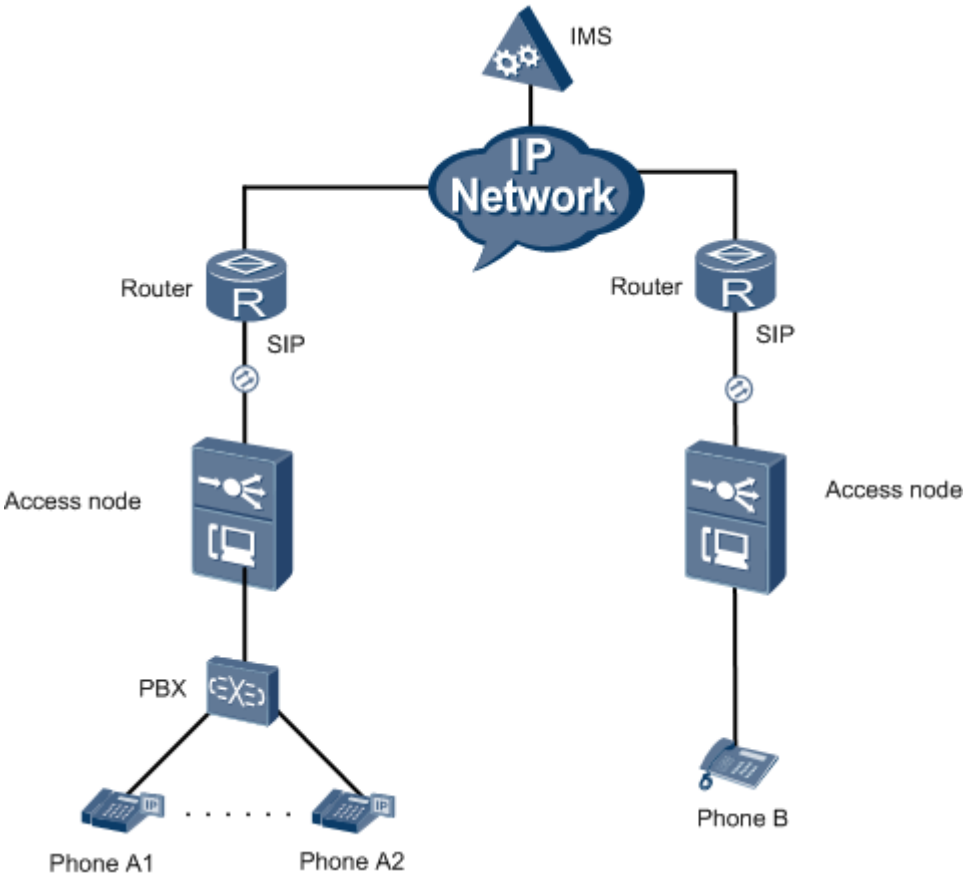
- The PBX is connected to the MA5600T/MA5603T/MA5608T through the ISDN PRI. PRI supports a data rate of 2048 kbit/s, including 30 B channels and one D channel. The rate of both the B channel and the D channel is 64 kbit/s.
- After the configuration is completed, users of the PBX can make calls successfully and can communicate with users outside the PBX in the normal state.

Networking

Figure 3-18 shows an example of the ISDN PRA service.

Copyright © Huawei Technologies Co., Ltd.

Figure 3-18 Example of the ISDN PRA service



Data Plan

Table 3-12 provides the data plan for configuring the ISDN PRA service.

Table 3-12 Data plan for configuring the ISDN PRA service

Item		Data
MG interface ID		0
ISDN PRA port	Subrack ID/Slot ID/Port ID	0/2/0
	Phone number	12345600

Procedure

Step 1 Configure the ISDN PRA user data.

```
huawei(config)#esl user
huawei(config-esl-user)#sipprauser add 0/2/0 0 telno 12345600
huawei(config-esl-user)#quit
```


Copyright © Huawei Technologies Co., Ltd.

Step 2 Save the data.

```
huawei(config)#save
```

----End

Result

After the configuration is completed, all the users of the PBX can communicate with Phone B in the normal state.

Configuration File

```
board add 0/2 H802EDTB
board confirm 0/2 H802EDTB
esl user
sipprauser add 0/2/0 0 telno 12345600
quit
save
```

3.3.11 Example: Configuring TDM SHDSL for Carrying the PRA Service

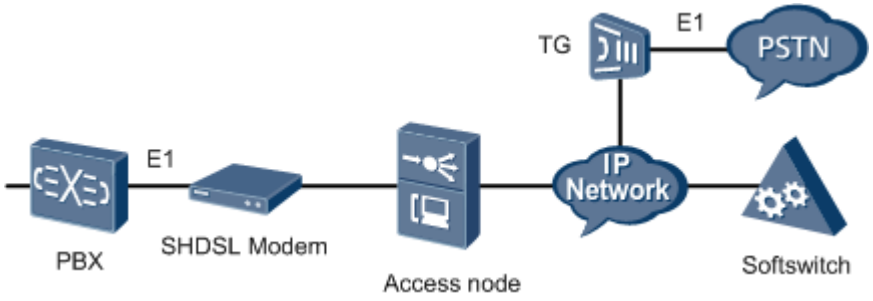
The MA5600T/MA5603T/MA5608T is connected to the PBX in the TDM SHDSL mode and then connected upstream to the IP network in the GE mode.

Service Requirements

- The PBX is connected to the IP network over a long distance to carry the PRA service.
- The user interface data is transparently transmitted on the MA5600T/MA5603T/MA5608T.

The following figure shows an example network of TDM SHDSL for carrying the PRA service.

Figure 3-19 Example network of TDM SHDSL for carrying the PRA service



Data Plan

The following table lists the data plan for configuring TDM SHDSL for carrying the PRA service.

Copyright © Huawei Technologies Co., Ltd.

Table 3-13 Data plan for configuring TDM SHDSL for carrying the PRA service

Item		Data
Clock source		E1 line clock on port 0/3/0
SHDSL port		Port ID: 0/3/16
IUA link set parameter	IUA link set ID	1
	Working mode of a link set	override
	Pending time	10s
	Mode of generating the interface ID	2
	Whether the link in the link set supports the interlocking	enable
	Service environment corresponding to the IUA link set	client
IUA link parameter	IUA link ID	15
	Local port ID	1401
	Local IP address	10.13.4.116/16 (It must exist in the signaling IP address pool.)
	Remote port ID	1400
	IP address of the primary MGC	10.14.1.2/16 (IP address of the primary MGC)
	MGC that is bound to the IUA link	primary-mgc
	Priority of the IUA link	3
	IP address of the primary MGC	10.14.1.2/16 (IP address of the primary MGC)
PRA user interface data		MGID: 0 IUA link set ID: 0 Terminal ID: 0

Prerequisite

- The H802EDTB board must be in position and must work in the normal state.

Copyright © Huawei Technologies Co., Ltd.

- An MG interface must be created and must communicate with the MGC in the normal state.
- An SHDSL modem must be correctly connected and the SHDSL port(s) must be activated.

Procedure

Step 1 (Optional) Configure the working mode of the board

Configure the working mode of the board to voice.

NOTE

The working sub-mode of the board can be configured only when the working mode of the board is configured to voice. By default, the working mode of the board is voice.

```
huawei(config)#interface edt 0/3
huawei(config-edt-0/3)#board workmode voice
```

Step 2 (Optional) Configure the working sub-mode of the board.

According to the service requirement, configure the working sub-mode of the board to service mode. By default, the working sub-mode of the board is service.

```
huawei(config-edt-0/3)#runmode service
```

Step 3 (Optional) Configure the clock source of the board.

Configure the E1 line clock on port 0/3/0 as the clock source.

NOTE

You can select the line clock or system clock as the clock source of the board according to your requirements. By default, the system clock is used as the clock source.

```
huawei(config-edt-0/3)#set clockmode line 0
```

Step 4 Configure the attributes of the SHDSL port.

Configure the signaling mode of SHDSL port 0/3/16 to CCS. PRA D channel signaling is transmitted in timeslot 16 and timeslot 0 is used for frame synchronization.

```
huawei(config-edt-0/3)#shdslport signal 16 CCS
huawei(config-edt-0/3)#quit
```

Step 5 Add an IUA link set and IUA links.

In the SIGTRAN mode, configure the SIGTRAN protocol stack. Add an IUA link set, and then add IUA links.

```
huawei(config)#sigtran
huawei(config-sigtran)#iua-linkset add 1 mgid 0 jointly-work enable trafficmode
override
iid-map 2 pendingtime cs-mode client
huawei(config-sigtran)#iua-link add 15 1 1401 10.13.4.116 1400 10.14.1.2
jointly-work-with primary-mgc priority 3
```

NOTE

All the ISDN call control messages are sent from the IUA link to the softswitch, whereas the system uses the bearer control messages to communicate with the softswitch through H.248.

Step 6 Configure a PRA user.

```
huawei(config)#esl user
huawei(config-esl-user)#mgprauser add 0/3/16 0 0 terminalid 0
huawei(config-esl-user)#quit
```

Step 7 Save the data.

```
huawei(config)#save
```

----End

Copyright © Huawei Technologies Co., Ltd.

Result

The phone set connected to the PBX can communicate with a phone set in the PSTN network in the normal state.

Configuration File

```
interface edt 0/3
board workmode voice
runmode service
set clockmode line 0
shdslport signal 16 CCS
quit
huawei(config)#sigtran
huawei(config-sigtran)#iua-linkset add 1 mgid 0 jointly-work enable trafficmode
override
iid-map 2 pendingtime cs-mode client
huawei(config-sigtran)#iua-link add 15 1 1401 10.13.4.116 1400 10.14.1.2
jointly-work-with primary-mgc priority 3
esl user
mgprauser add 0/3/16 0 0 terminalid 0
quit
save
```

3.3.12 Example: Configuring TDM SHDSL for Carrying the PRA Service (Based on the SIP Protocol)

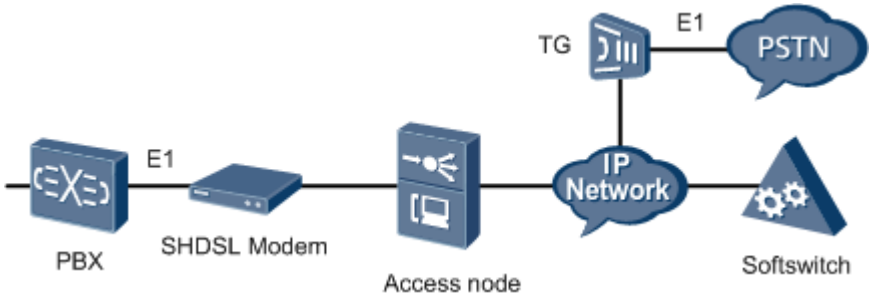
The MA5600T/MA5603T/MA5608T is connected to the PBX in the TDM SHDSL mode and then connected upstream to the IP network in the GE mode.

Service Requirements

- The PBX is connected to the IP network over a long distance to carry the PRA service.
- The configuration data is transparently transmitted on the MA5600T/MA5603T/MA5608T.

The following figure shows an example network of TDM SHDSL for carrying the PRA service.

Figure 3-20 Example network of TDM SHDSL for carrying the PRA service



Data Plan

The following table lists the data plan for configuring TDM SHDSL for carrying the PRA service.

Copyright © Huawei Technologies Co., Ltd.

Table 3-14 Data plan for configuring TDM SHDSL for carrying the PRA service

Item	Data
Clock source	E1 line clock on port 0/3/0
SHDSL port	Port ID: 0/3/16
PRA user interface data	MGID: 0 IUA link set ID: 0 Terminal ID: 0 Phone number: 12345600

Prerequisite

- The H802EDTB board must be in position and must work in the normal state.
- The MA5600T/MA5603T/MA5608T must use the SIP protocol to communicate with the IMS in the normao state.
- An SHDSL modem must be correctly connected and the SHDSL port(s) must be activated.

Procedure

Step 1 (Optional) Configure the working mode of the board

Configure the working mode of the board to voice.

NOTE

The working sub-mode of the board can be configured only when the working mode of the board is configured to voice. By default, the working mode of the board is voice.

```
huawei(config)#interface edt 0/3
huawei(config-edt-0/3)#board workmode voice
```

Step 2 (Optional) Configure the working sub-mode of the board.

According to the service requirement, configure the working sub-mode of the board to service mode. By default, the working sub-mode of the board is service.

```
huawei(config-edt-0/3)#runmode service
```

Step 3 (Optional) Configure the clock source of the board.

Configure the E1 line clock on port 0/3/0 as the clock source.

NOTE

You can select the line clock or system clock as the clock source of the board according to your requirements. By default, the system clock is used as the clock source.

```
huawei(config-edt-0/3)#set clockmode line 0
```

Step 4 Configure the attributes of the SHDSL port.

Configure the signaling mode of SHDSL port 0/3/16 to CCS. PRA D channel signaling is transmitted in timeslot 16 and timeslot 0 is used for frame synchronization.

```
huawei(config-edt-0/3)#shdslport signal 16 CCS
huawei(config-edt-0/3)#quit
```

Step 5 Configure a PRA user.

Copyright © Huawei Technologies Co., Ltd.

```
huawei(config)#esl user
huawei(config-esl-user)#sipprauser add 0/3/16 0 telno 12345600
huawei(config-esl-user)#quit
```

Step 6 Save the data.

```
huawei(config)#save
```

----End

Result

The phone set connected to the PBX can communicate with a phone set in the PSTN network in the normal state.

Configuration File

```
interface edt 0/3
board workmode voice
runmode service
set clockmode line 0
shdslport signal 16 CCS
quit
esl user
sipprauser add 0/3/16 0 telno 12345600
quit
save
```

3.3.13 Configuring VAGs

The purpose of configuring virtual access gateways (VAGs) is to simulate multiple AGs by using one AG, increasing the usage rate and flexibility of the device.

3.3.13.1 Example: Configuring the H.248/MGCP-based VAG Service

This topic describes how to configure the VAG service by creating two MG interfaces on the MA5600T/MA5603T/MA5608T and configuring PSTN users on the two MG interfaces. This topic is applicable to the scenario where multiple logical AGs are simulated on one physical AG.

Context

Configuring VAGs is literally to configure MG interfaces with different IDs on the same device, and to configure user ports homing to different MG interfaces. Pay attention to the following points:

- When the system uses the MGCP or H.248 protocol, up to eight MG interfaces with different IDs can be configured on the MA5600T/MA5603T/MA5608T, and each MG interface can be considered as a VAG.
- When configuring the parameters for interconnecting different MG interfaces with the MGC, make sure that the values of the following parameters of the MG interfaces are not the same. The values of at least one of the following parameters must be different on the MG interfaces.
  - Local IP address
  - Local port ID
  - Remote IP address

Copyright © Huawei Technologies Co., Ltd.

- Remote port ID

Service Requirements

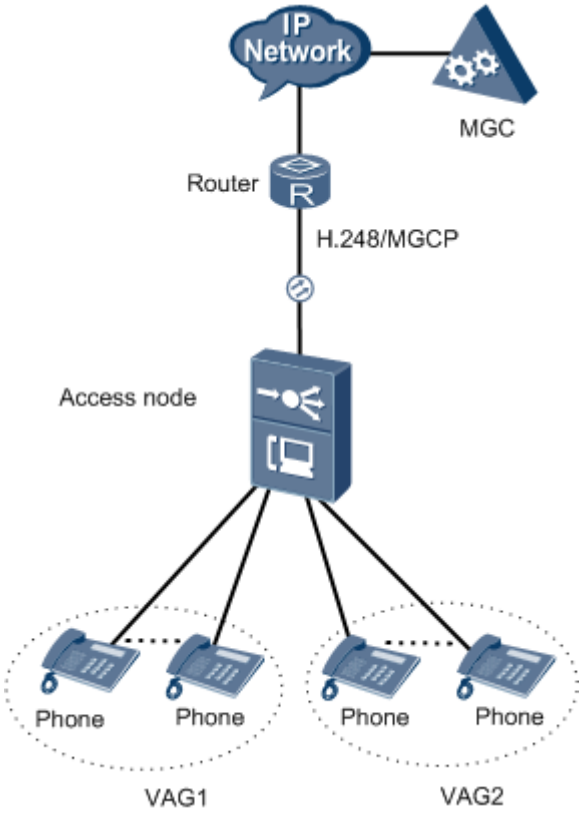
The service requirements are as follows:

- As shown in **Figure 3-21**, configure VAG1, and configure the users in slot 0/2 to belong to VAG1; configure VAG2, and configure the users in slot 0/3 to belong to VAG2.
- The MG communicates with the MGC through the H.248 protocol.
- Configure the data plan of VAG1 as listed in **Table 3-15**.
- The data plan of VAG2 is the same as that of VAG1 except for the following differences:
  - The media IP address and signaling IP address of VAG2 are 10.10.10.11.
  - The MGC assigns phone numbers 85110000-85110031 to phones 0-31 of VAG2.
- MG0 indicates VAG1 in the figure, and MG1 indicates VAG2 in the figure.

Networking

Figure 3-21 shows an example network of the VAG service.

Figure 3-21 Example network of the VAG service



Copyright © Huawei Technologies Co., Ltd.

Dataplan

Table 3-15 Data plan of VAG1

Item			Data
MG interface data (The data configuration must be the same as the data configuration on the MGC.)	Media and signaling parameters	Media and signaling upstream VLAN	Standard VLAN is recommended as the upstream VLAN of the voice service. Standard VLAN 20 is adopted.
		Media and signaling upstream port	In this office, all the services are transmitted upstream through the upstream interface board. Therefore, port 0/19/0 is used as the upstream port of the voice service.
		Media IP address and signaling IP addresses	These two IP addresses are both 10.10.10.10.
		Default gateway IP address	The IP address of the next hop from the MA5600T/MA5603T/MA5608T to the MGC is 10.10.10.1.
	Attributes of the MG interface **NOTE** Parameters listed here are mandatory, which means that the MG interface fails to be enabled if these parameters are not configured.	MG interface ID	0 and 1
		Signaling port ID of the MG interface	2944
		IP address of the primary MGC to which the MG interface belongs	The IP address of the primary MGC is 10.10.20.20, and the port ID is 2944, the same as the port ID on the MA5600T/MA5603T/MA5608T.
		Port ID of the primary MGC to which the MG interface belongs	
		Coding mode of the MG interface	**text** (indicates the text coding mode)
		Transmission mode of the MG interface	UDP

Copyright © Huawei Technologies Co., Ltd.

Item			Data
	(Optional) Configuring the TID Format of an MG Interface		To differentiate users according to the TID, the office requires that the terminal prefix uses the community name **huawei** and the TID is automatically generated by the system according to the subrack ID/slot ID/port ID (F/S/P) of the user. Run the **display tid-template** command to query the default TID template. It is found that default TID template (template 6) can meet the requirements.
Voice user data (The data configuration must be the same as the data configuration on the MGC.)	Slot of the voice service board		User access is implemented by the ASPB board in slot 0/2 and 0/3.
	Configuring the PSTN User Data	Phone number	The emergency standalone is not supported, and therefore the phone numbers do not need to be configured when the users are added. The MGC assigns phone numbers 83110000-83110031 to phones 0-31.
		TID	The terminal layering is supported, and therefore the TIDs do not need to be allocated manually.

Procedure

- Configure VAG1.
  1. Add the upstream VLAN interface.

     According to the data plan, configure standard VLAN 20 as the media and signaling upstream VLAN, add upstream port 0/19/0 to the VLAN, and configure the IP address of the Layer 3 interface to 10.10.10.10, which facilitates the configuration of the media and signaling IP address pools.

     ```
     huawei(config)#vlan 20 standard
     huawei(config)#port vlan 20 0/19 0
     huawei(config)#interface vlanif 20
     huawei(config-if-vlanif20)#ip address 10.10.10.10 24
     huawei(config-if-vlanif20)#quit
     ```

  2. Configure the media and signaling IP address pools.

     Add the IP address of the VLAN Layer 3 interface configured in the previous step to the media and signaling IP address pools respectively. Therefore, the media and signaling IP addresses used for the services can be selected from the IP address pools. According to the data plan, IP address 10.10.10.10 is added to the media and signaling IP address pools, and the gateway IP address corresponding to the media IP address is 10.10.10.1.

Copyright © Huawei Technologies Co., Ltd.

```
huawei(config)#voip
huawei(config-voip)#ip address media 10.10.10.10 10.10.10.1
huawei(config-voip)#ip address signaling 10.10.10.10
huawei(config-voip)#quit
```

3. Add an MG interface.

   Add an MG interface for the MG to communicate with the MGC, which ensures that the MGC can control the call connection through the MG interface. According to the data plan, add MG interface 0, and configure the interface attributes.

```
huawei(config)#interface h248 0
  Are you sure to add MG interface?(y/n)[n]:y
huawei(config-if-h248-0)#if-h248 attribute mg-media-ip1 10.10.10.10 mgip
10.10.10.10 mgport 2944 primary-mgc-ip1 10.10.20.20
primary-mgc-port 2944 code text transfer udp
```

4. Configure the TID template of the PSTN users on MG interface 0.

   Configure the TID generation mode. According to the data plan, the terminal prefix of PSTN users is **huawei**, and the TID template adopts layering template 6.

NOTICE

The MA5600T/MA5603T/MA5608T requires that the terminal prefixes of PSTN users, ISDN BRA users, and ISDN PRA users on the same H.248 interface be either the same or different. Note this when configuring the terminal prefix.

```
huawei(config-if-h248-0)#tid-format pstn prefix huawei template 6
```

5. Reset the MG interface.

   Reset the MG interface to make the MG interface register with the MGC (and to make the modified attributes of the MG interface take effect) so that the MG interface can work in the normal state. The MG interface can be started in different ways (see Parameters of the **reset** command). For a newly configured MG interface, enable the MG interface through cold start.

```
huawei(config-if-h248-0)#reset coldstart
  Are you sure to reset MG interface?(y/n)[n]:y
huawei(config-if-h248-0)#quit
```

6. Query the running status of the MG interface.

   After the MG interface is interconnected with the MGC, the MG interface should be in the normal state, indicating that the MG interface works in the normal state.

```
huawei(config)#display if-h248 all

------------------------------------------------------------------------
-----
  MGID     Trans State           MGPort MGIP            MGCPort MGCIP/
DomainName

------------------------------------------------------------------------
-----
  0        UDP   Normal          2944   10.10.10.10     2944
10.10.20.20

------------------------------------------------------------------------
-----
```


Copyright © Huawei Technologies Co., Ltd.

7. Confirm the service board.

   Confirm the ASPB service board that carries services so that the board can work in the normal state.

   ```
   huawei(config)#board confirm 0/2
   ```

8. Configure the PSTN user data.

   Add POTS users (phones 0-31) so that the users can go online.

   ```
   huawei(config)#esl user
   huawei(config-esl-user)#mgpstnuser batadd 0/2/0 0/2/31 0
   huawei(config-esl-user)#quit
   ```

9. Save the data.

   ```
   huawei(config)#save
   ```

- Configure VAG2.

  1. Add the upstream VLAN interface.

     According to the data plan, configure the secondary IP address of the Layer 3 interface to 10.10.10.11, which facilitates the configuration of the media and signaling IP address pools.

     In step **Step 1**, the VLAN is added and the IP address of the VLAN Layer 3 interface is configured. In this step, use the sub parameter to configure the secondary IP address of the VLAN. The secondary IP address is the same as the primary IP address in function. They are used for Layer 3 forwarding.

     ```
     huawei(config)#interface vlanif 20
     huawei(config-if-vlanif20)#ip address 10.10.10.11 24 sub
     huawei(config-if-vlanif20)#quit
     ```

  2. Configure the media and signaling IP address pools.

     Add the IP address of the VLAN Layer 3 interface configured in the previous step to the media and signaling IP address pools respectively. Therefore, the media and signaling IP addresses used for the services can be selected from the IP address pools. According to the data plan, IP address 10.10.10.11 is added to the media and signaling IP address pools, and the gateway IP address corresponding to the media IP address is 10.10.10.1.

     ```
     huawei(config)#voip
     huawei(config-voip)#ip address media 10.10.10.11 10.10.10.1
     huawei(config-voip)#ip address signaling 10.10.10.11
     huawei(config-voip)#quit
     ```

  3. Add an MG interface.

     Add an MG interface for the MG to communicate with the MGC, which ensures that the MGC can control the call connection through the MG interface. According to the data plan, add MG interface 1, and configure the interface attributes.

     ```
     huawei(config)#interface h248 1
       Are you sure to add MG interface?(y/n)[n]:y
     huawei(config-if-h248-1)#if-h248 attribute mg-media-ip1 10.10.10.11 mgip
     10.10.10.11 mgport 2944 primary-mgc-ip1 10.10.20.20
     primary-mgc-port 2944 code text transfer udp
     ```

  4. Configure the TID template of the PSTN users on MG interface 1.

     Configure the TID generation mode. According to the data plan, the terminal prefix of PSTN users is **huawei**, and the TID template adopts layering template 6.

Copyright © Huawei Technologies Co., Ltd.

NOTICE

The MA5600T/MA5603T/MA5608T requires that the terminal prefixes of PSTN users, ISDN BRA users, and ISDN PRA users on the same H.248 interface be either the same or different. Note this when configuring the terminal prefix.

```
huawei(config-if-h248-1)#tid-format pstn prefix huawei template 6
```

5. Reset the MG interface.

   Reset the MG interface to make the MG interface register with the MGC (and to make the modified attributes of the MG interface take effect) so that the MG interface can work in the normal state. The MG interface can be started in different ways (see Parameters of the **reset** command). For a newly configured MG interface, enable the MG interface through cold start.

```
huawei(config-if-h248-1)#reset coldstart
  Are you sure to reset MG interface?(y/n)[n]:y
huawei(config-if-h248-1)#quit
```

6. Query the running status of the MG interface.

   After the MG interface is interconnected with the MGC, the MG interface should be in the normal state, indicating that the MG interface works in the normal state.

```
huawei(config)#display if-h248 all

------------------------------------------------------------------------------
  MGID     Trans State           MGPort MGIP            MGCPort MGCIP/
DomainName

------------------------------------------------------------------------------
   0        UDP   Normal          2944   10.10.10.10     2944
10.10.20.2
   1        UDP   Normal          2944   10.10.10.11     2944
10.10.20.20

------------------------------------------------------------------------------
```

7. Confirm the service board.

   Confirm the ASPB service board that carries services so that the board can work in the normal state.

```
huawei(config)#board confirm 0/3
```

8. Configure the PSTN user data.

   Add POTS users (phones 0-31) so that the users can go online.

```
huawei(config)#esl user
huawei(config-esl-user)#mgpstnuser batadd 0/3/0 0/3/31 1
huawei(config-esl-user)#quit
```

9. Save the data.

```
huawei(config)#save
```

----End

Copyright © Huawei Technologies Co., Ltd.

Result

1. When MG0 communicates with the MGC in the normal state, phones 0-31 belonging to MG0 can communicate with each other.
2. When MG1 communicates with the MGC in the normal state, phones 0-31 belonging to MG1 can communicate with each other.
3. When MG0 and MG1 communicate with the MGC in the normal state, phones 0-31 belonging to MG0 and phones 0-31 belonging to MG1 can communicate with each other.

3.3.13.2 Example: Configuring the SIP-based VAG Service

This topic describes how to configure and verify the VAG service by creating two SIP interfaces on the MA5600T/MA5603T/MA5608T and configuring PSTN users on the two SIP interfaces. This topic is applicable to the scenario where multiple logical AGs are simulated on one physical SIP AG.

Context

Configuring VAGs is literally to configure SIP interfaces with different IDs on the same device, and to configure user ports homing to different SIP interfaces. Pay attention to the following points:

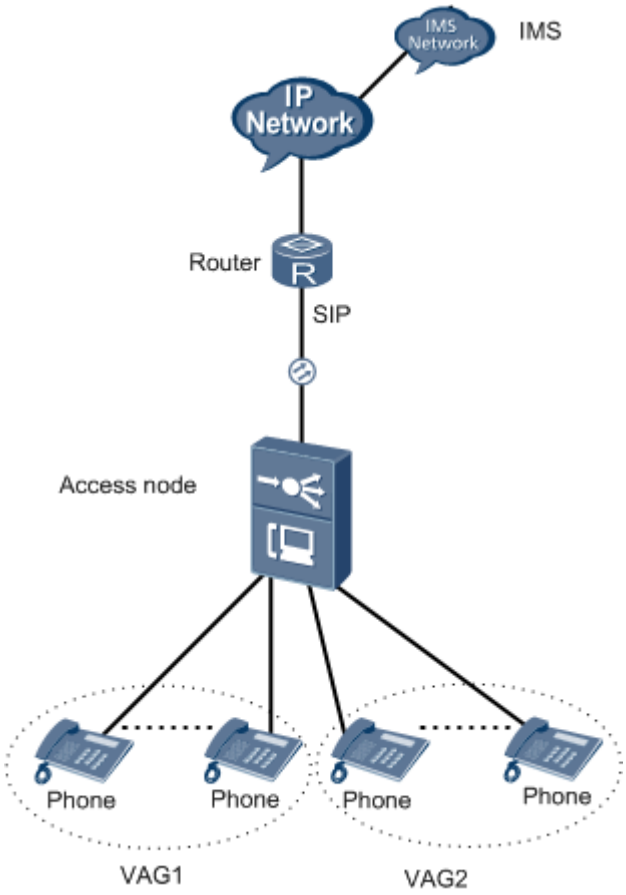
- When the system uses the SIP protocol, up to eight SIP interfaces with different IDs can be configured on the MA5600T/MA5603T/MA5608T, and each SIP interface can be considered as a VAG.
- When configuring the parameters for interconnecting different SIP interfaces with the IMS, make sure that the values of the following parameters of the SIP interfaces are not completely the same. The values of at least one of the following parameters must be different on the SIP interfaces.
  - Local IP address
  - Local port ID
  - Remote IP address
  - Remote port ID

Service Requirements

Figure 3-22 shows an example network of the SIP-based VAG service.

Copyright © Huawei Technologies Co., Ltd.

Figure 3-22 Example network of the SIP-based VAG service



Data Plan

The service requirements are as follows:

- As shown in **Figure 3-22**, configure VAG1, and configure the users in slot 0/2 to belong to VAG1; configure VAG2, and configure the users in slot 0/3 to belong to VAG2.
- The MA5600T/MA5603T/MA5608T communicates with the IMS through the SIP protocol.
- Configure the data plan of VAG1 as listed in **Table 3-16**.
- The data plan of VAG2 is the same as that of VAG1 except for the following differences:
  - The media IP address and signaling IP address of VAG2 are 10.20.10.11.
  - The IMS assigns phone numbers 85000000-85000031 to phones 0-31 of VAG2.
- SIP interface 0 indicates VAG1 in the figure, and SIP interface 1 indicates VAG2 in the figure.

Copyright © Huawei Technologies Co., Ltd.

Table 3-16 Data plan of VAG1

Item			Remarks
SIP interface data (The data configuration must be the same as the data configuration on the IMS.)	Media and signaling parameters	Media and signaling upstream VLAN	Standard VLAN 30 is adopted.
		Media and signaling upstream port	In this office, all the services are transmitted upstream through the control board. Therefore, port 0/19/0 is used as the upstream port of the voice service.
		Media IP address and signaling IP addresses	These two IP addresses are both 10.20.10.10.
		Default gateway IP address	The IP address of the next hop from the MA5600T/MA5603T/MA5608T to the IMS core network device is 10.20.10.1.
	Attributes of the SIP interface **NOTE** Parameters listed here are mandatory, which means that the SIP interface fails to be enabled if these parameters are not configured.	SIP interface ID	0 and 1
		Signaling port ID of the SIP interface	5060
		IP address of the primary IMS core network device to which the SIP interface belongs	10.20.20.100
		Port ID of the primary IMS core network device to which the SIP interface belongs	5060
		Transmission mode of the SIP interface	UDP
		Homing domain name of the SIP interface	huawei
		Index of the profile used by the SIP interface	Default profile (profile 1)
Voice user data (The data configuration	Slot of the voice service board		The ASPB service board in slot 0/2 and 0/3.

Copyright © Huawei Technologies Co., Ltd.

Item		Remarks
must be the same as the data configuration on the IMS.)	Phone number	80000000-80000031

Procedure

- Configure VAG1.
  1. Add the upstream VLAN interface.

     According to the data plan, configure standard VLAN 30 as the media and signaling upstream VLAN, add upstream port 0/19/0 to the VLAN, and configure the IP address of the Layer 3 interface to 10.20.10.10, which facilitates the configuration of the media and signaling IP address pools.

     ```
     huawei(config)#vlan 30 standard
     huawei(config)#port vlan 30 0/19 0
     huawei(config)#interface vlanif 30
     huawei(config-if-vlanif30)#ip address 10.20.10.10 24
     huawei(config-if-vlanif30)#quit
     ```

  2. Configure the media and signaling IP address pools.

     Add the IP address of the VLAN Layer 3 interface configured in the previous step to the media and signaling IP address pools respectively. Therefore, the media and signaling IP addresses used for the services can be selected from the IP address pools. According to the data plan, IP address 10.20.10.10 is added to the media and signaling IP address pools, and the gateway IP address corresponding to the media IP address is 10.20.10.1.

     ```
     huawei(config)#voip
     huawei(config-voip)#ip address media 10.20.10.10 10.20.10.1
     huawei(config-voip)#ip address signaling 10.20.10.10
     huawei(config-voip)#quit
     ```

  3. Configure a static route to the IMS.

     Make sure that the route between the local device and the IMS is reachable. The static route is used as an example.

     ```
     huawei(config)#ip route-static 10.20.0.0 255.255.0.0 10.20.10.1
     ```

  4. Add a SIP interface.

     According to the data plan, add SIP interface 0, and configure the interface attributes.

     ```
     huawei(config)#interface sip 0
       Are you sure to add the SIP interface?(y/n)[n]:y
     huawei(config-if-sip-0)#if-sip attribute basic media-ip 10.20.10.10
     signal-ip
     10.20.10.10 signal-port 5060 transfer udp primary-proxy-ip1 10.20.20.100
     primary-proxy-port 5060
      home-domain huawei sipprofile-index 1
     ```

  5. Reset the SIP interface.

     Reset the SIP interface to make the SIP interface register with the IMS (and to make the modified attributes of the SIP interface take effect) so that the SIP interface can work in the normal state.

Copyright © Huawei Technologies Co., Ltd.

```
huawei(config-if-sip-0)#reset
  Are you sure to reset SIP interface?(y/n)[n]:y
```

6. Confirm the service board.

   Confirm the ASPB service board that carries services so that the board can work in the normal state.

   ```
   huawei(config)#board confirm 0/2
   ```

7. Configure the PSTN user data.

   Add POTS users (phones 0-31) to VAG1 so that the users can go online.

   ```
   huawei(config)#esl user
   huawei(config-esl-user)#sippstnuser batadd 0/2/0 0/2/31 0 telno 80000000
   huawei(config-esl-user)#quit
   ```

8. Save the data.

   ```
   huawei(config)#save
   ```

- Configure VAG2.

1. Add the upstream VLAN interface.

   According to the data plan, configure the IP address of the Layer 3 interface to 10.20.10.11, which facilitates the configuration of the media and signaling IP address pools.

   When you need to connect the VLAN interface to multiple subnets and configure the secondary IP address, use **sub** parameter. The secondary IP address is the same as the primary IP address in function. They are used for Layer 3 forwarding.

   In step **Step 1**, the VLAN is added and the IP address of the VLAN Layer 3 interface is configured. In this step, use the sub parameter to configure the secondary IP address of the VLAN. The secondary IP address is the same as the primary IP address in function. They are used for Layer 3 forwarding.

   ```
   huawei(config)#interface vlanif 30
   huawei(config-if-vlanif30)#ip address 10.20.10.11 24 sub
   huawei(config-if-vlanif30)#quit
   ```

2. Configure the media and signaling IP address pools.

   Add the IP address of the VLAN Layer 3 interface configured in the previous step to the media and signaling IP address pools respectively. Therefore, the media and signaling IP addresses used for the services can be selected from the IP address pools. According to the data plan, IP address 10.20.10.11 is added to the media and signaling IP address pools, and the gateway IP address corresponding to the media IP address is 10.20.10.1.

   ```
   huawei(config)#voip
   huawei(config-voip)#ip address media 10.20.10.11 10.20.10.1
   huawei(config-voip)#ip address signaling 10.20.10.11
   huawei(config-voip)#quit
   ```

3. Configure a static route to the IMS.

   Make sure that the route between the local device and the IMS is reachable. The static route is used as an example. If the static route has been configured, skip this step.

   ```
   huawei(config)#ip route-static 10.20.0.0 255.255.0.0 10.20.10.1
   ```

4. Add a SIP interface.

   According to the data plan, add SIP interface 1, and configure the interface attributes.

Copyright © Huawei Technologies Co., Ltd.

```
huawei(config)#interface sip 1
  Are you sure to add the SIP interface?(y/n)[n]:y
huawei(config-if-sip-1)#if-sip attribute basic media-ip 10.20.10.11
signal-ip
10.20.10.11 signal-port 5060 transfer udp primary-proxy-ip1 10.20.20.100
primary-proxy-port 5060
 home-domain huawei sipprofile-index 1
```

5. Reset the SIP interface.

   Reset the SIP interface to make the SIP interface register with the IMS (and to make the modified attributes of the SIP interface take effect) so that the SIP interface can work in the normal state.

   ```
   huawei(config-if-sip-1)#reset
       Are you sure to reset SIP interface?(y/n)[n]:y
   ```

6. Confirm the service board.

   Confirm the ASPB service board that carries services so that the board can work in the normal state.

   ```
   huawei(config)#board confirm 0/3
   ```

7. Configure the PSTN user data.

   Add POTS users (phones 0-31) to VAG2 so that the users can go online.

   ```
   huawei(config)#esl user
   huawei(config-esl-user)#sippstnuser batadd 0/3/0 0/3/31 1 telno 85000000
   huawei(config-esl-user)#quit
   ```

8. Save the data.

   ```
   huawei(config)#save
   ```

----End

Result

After the configuration:

- Users of VAG1 can communicate with each other.
- Users of VAG2 can communicate with each other.
- Users of VAG1 and VAG2 can communicate with each other.

3.4 Example: Configuring the Triple Play

This topic describes how to configure the Triple Play on the MA5600T/MA5603T/MA5608T.

Triple play is a service provisioning mode in which integrated services can be provided to a user. Currently, the prevailing integrated services include the high-speed Internet access service, voice over IP (VoIP) service, and IPTV service.

The early broadband access provides only the high-speed Internet access service. As the Internet is rapidly developing, it can offer much richer services, such as video (IPTV) services. The development of multiple access modes such as ADSL2+ and VDSL2 access, and the improvement of broadband access also lay a solid foundation for provisioning the video service.

Copyright © Huawei Technologies Co., Ltd.

PVC Modes for Triple Play Implementation

MA5600T/MA5603T/MA5608T supports the triple play implemented in single-PVC multiple services and multi-PVC multiple services modes.

PVC Mode	Implementation	Application Scenario
Single-PVC for single service	Single-PVC for single service is a triple play mode in which a PVC is adopted for carrying one type of service.	This mode provides only the Internet access service and is used only in early days.
Multi-PVC for multiple services	Multi-PVC for multiple services is a triple play mode in which multiple PVCs are adopted for carrying multiple services from the MA5600T/MA5603T/MA5608T to each DSL user terminal. ● On the user side, three PVCs are used for carrying VoIP, IPTV, and Internet services, and each xDSL port must be configured with at least three PVCs. ● At the network end, three VLANs are created for the upstream interface to carry different types of services.	The home gateway differentiates services based on PVCs. This mode is adopted to utilize the previously-configured services and previously-deployed user terminals.
Single-PVC for multiple services	Single-PVC for multiple services is a triple play mode in which a single PVC is adopted for carrying multiple services from the MA5600T/MA5603T/MA5608T to each DSL user terminal. The MA5600T/MA5603T/MA5608T can differentiate services by the following means: ● Ethernet type (IPoE/PPPoE) ● User-side VLAN ID ● User-side 802.1p value ● 802.1p value + VLAN ID carried in the Ethernet packet ● Ethernet type (IPoE/PPPoE) + VLAN ID	The home gateway differentiates services based on Ethernet parameters such as such as the VLAN ID or the 802.1p priority. This mode is recommended if the home gateway supports the preceding function.

Service Priorities and Bandwidth

The different services have different request on the bandwidth and priority.

- Because the bandwidth and delay of the VoIP service are low, the priority of the VoIP service is the highest among the triple play services.

Copyright © Huawei Technologies Co., Ltd.

- Because the bandwidth occupied by the IPTV service is relatively high, and the bit error ratio/packet loss ratio is relatively low, the priority of the IPTV service is lower than that of the VoIP service, but is higher than that of the Internet access service.
- Because common Internet access services, such as web browsing, require neither a strong real-time performance nor a low packet loss ratio, the priority of the high-speed Internet access service is the lowest among the triple play services.

Traffic Management for the Triple Play Services

Traffic management for the triple play includes two modes of rate limitations: stream-based and user (xDSL port)-based. These two modes are implemented on different layers, and therefore can be used together. When implementing the user (xDSL port)-based rate limitation, ensure that the rate limit for the user (xDSL port) must be higher than the aggregated rate limits for all services of the user.

- The stream-based rate limitation

  The stream-based rate limitation is planned based on services, for example, the bandwidth is planned based on the IPTV HD program and the IPTV SD program.
- The user (xDSL port)-based rate limitation

  The user (xDSL port)-based rate limitation is planned based on physical information, such as line quality and number of users per port. The bandwidth for each user is managed in a unified way: Every users' VoIP, IPTV, and Internet services share one user bandwidth, the bandwidth is preferentially allocated to the service with higher priority, and one service burst can hold the total user bandwidth when the other two services carry no traffic.

3.4.1 Configuration Example of the Triple Play (Multi-PVC for Multiple Services)

This topic describes how to configure the triple play in the multi-PVC for multiple services mode. The user home gateway is connected to multiple terminals to implement the access of multiple services such as Internet access service, VoIP service, and IPTV service. Carriers can adopt this mode when they want to use the existing operation, maintenance, and management system for the triple play services.

Prerequisites

- Network devices and lines must be in the normal state.
- The system is working properly.
- The home gateway has been configured. Specifically, permanent virtual channels (PVCs) have been configured on the home gateway for different services.
- The asymmetric digital subscriber line 2 plus (ADSL2+) line template and alarm template that need to be bound to ports have been configured.

Service Requirements

ADSL2+ user 1 and ADSL2+ user 2 are connected to the MA5600T/MA5603T/MA5608T to implement the triple play.

- The PC user accesses the Internet properly.

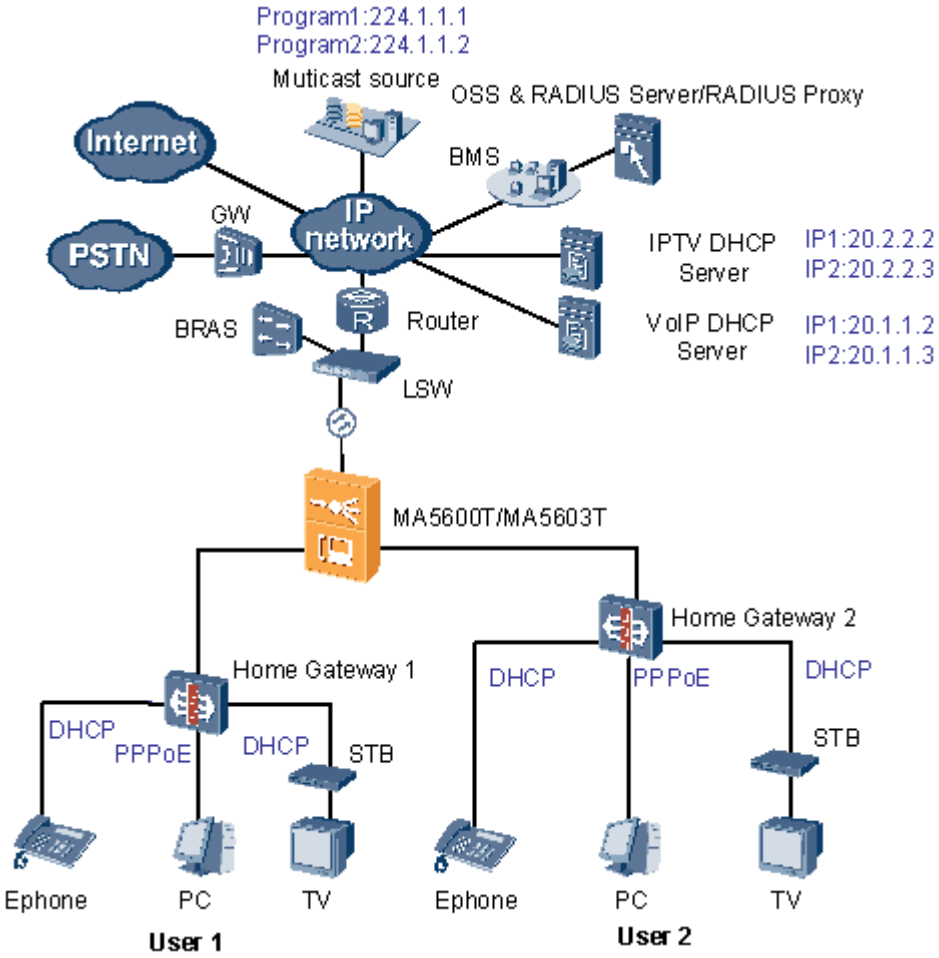
Copyright © Huawei Technologies Co., Ltd.

- The VoIP user makes calls properly.
- The IPTV user watches programs properly.
- After receiving different traffic streams, the MA5600T/MA5603T/MA5608T provides different QoS guarantees to the traffic streams according to the traffic priorities of the PVC.

Networking

Figure 3-23 shows an example network of the triple play service in the multi-PVC for multiple services mode. The Internet service is provided in the PPPoE mode. The VoIP service and the IPTV service are provided in the DHCP mode, obtaining IP addresses from the DHCP server in the standard DHCP mode.

Figure 3-23 Example network of the triple play service in the multi-PVC for multiple services mode



Data Plan

Table 3-17 shows the key data for configuring the triple play in multi-PVC for multiple services mode on the MA5600T/MA5603T/MA5608T.

Copyright © Huawei Technologies Co., Ltd.

Table 3-17 Data plan for configuring the triple play in multi-PVC for multiple services mode

Configuration Item	Data			Remarks
	Internet access	VoIP	IPTV	
Upstream port	0/19 0			-
ADSL2+ port	● User 1: 0/2/1 ● User 2: 0/3/1			-
VLAN	● VLAN ID: 2 ● VLAN type: smart	● VLAN ID: 3 ● VLAN type: smart	● VLAN ID: 4 ● VLAN type: smart	-
Traffic profile	● Index: 7 ● CIR: 2 Mbit/s ● Default packet 802.1p priority: 1 ● Priority scheduling policy of downstream packets: Local-Setting	● Index: 8 ● CIR: 1 Mbit/s ● Default packet 802.1p priority: 6 ● Priority scheduling policy of downstream packets: Local-Setting	● Index: 9 ● No rate limitation ● Default packet 802.1p priority: 5 ● Priority scheduling policy of downstream packets: Local-Setting	As VoIP, IPTV, and Internet services access from the same port, the 802.1p priorities for each service must be configured. These three services are prioritized in descending order as follows: VoIP, IPTV, Internet access.
Service port	● VPI: 0 ● VCI: 37	● VPI: 0 ● VCI: 36	● Index: 100 and 101 ● VPI: 0 ● VCI: 35	The three services have different VCIs.

Copyright © Huawei Technologies Co., Ltd.

Configuration Item	Data			Remarks
	Internet access	VoIP	IPTV	
DHCP relay	-	● Number of the DHCP server group: 1 ● IP address of DHCP server group 1: 20.1.1.2 ● IP address of DHCP server group 2: 20.1.1.3 ● IP address of the VLAN Layer 3 interface: 10.1.1.1/24	● Number of the DHCP server group: 2 ● IP address of DHCP server group 1: 20.2.2.2 ● IP address of DHCP server group 2: 20.2.2.3 ● IP address of the VLAN Layer 3 interface: 10.2.2.1/24	-
Multicast	-	-	● Multicast mode: IGMP Proxy ● Profile 0 of multicast user 2: the right to watch only program BTV-1 ● Multicast upstream port: 0/19/0 ● Multicast IP address of program BTV-1: 224.1.1.1; program source IP address: 10.10.10.10 ● Multicast IP address of program BTV-2: 224.1.1.2; program source IP address: 10.10.10.10	-

Copyright © Huawei Technologies Co., Ltd.

Procedure

- Configure the Internet service.
  1. Create a VLAN and add an upstream port to the VLAN.

     ```
     huawei(config)#vlan 2 smart
     huawei(config)#port vlan 2 0/19 0
     ```

  2. Add a traffic profile.

     ```
     huawei(config)#traffic table ip index 7 cir 2048 priority 1 priority-policy local-Setting
     ```

  3. Add a service port to the VLAN.

     Add a service port to the VLAN 2 and use the traffic profile 7 added in the preceding step.

     ```
     huawei(config)#service-port vlan 2 adsl 0/2/1 vpi 0 vci 37 rx-cttr 7 tx-cttr 7
     huawei(config)#service-port vlan 2 adsl 0/3/1 vpi 0 vci 37 rx-cttr 7 tx-cttr 7
     ```

  4. Save the data.

     ```
     huawei(config)#save
     ```

- Configure the VoIP service.
  1. Create a VLAN and add an upstream port to the VLAN.

     ```
     huawei(config)#vlan 3 smart
     huawei(config)#port vlan 3 0/19 0
     ```

  2. Add a traffic profile.

     ```
     huawei(config)#traffic table ip index 8 cir 1024 priority 6 priority-policy local-Setting
     ```

  3. Add a service port to the VLAN.

     Add a service port to the VLAN 3 and use the traffic profile 8 added in the preceding step.

     ```
     huawei(config)#service-port vlan 3 adsl 0/2/1 vpi 0 vci 36 rx-cttr 8 tx-cttr 8
     huawei(config)#service-port vlan 3 adsl 0/3/1 vpi 0 vci 36 rx-cttr 8 tx-cttr 8
     ```

  4. Configure the DHCP relay.

     Configure the IP addresses of DHCP server 1 and the IP address of the VLAN Layer 3 interface, and bind the VLAN Layer 3 interface to DHCP server 1.

     ```
     huawei(config)#dhcp mode layer-3 standard
     huawei(config)#dhcp-server 1 ip 20.1.1.2 20.1.1 3
     huawei(config)#interface vlanif 3
     huawei(config-if-vlanif3)#ip address 10.1.1.1 24
     huawei(config-if-vlanif3)#dhcp-server 1
     huawei(config-if-vlanif3)#quit
     ```

  5. Save the data.

     ```
     huawei(config)#save
     ```

- Configure the IPTV service.
  1. Create a VLAN and add an upstream port to the VLAN.

     ```
     huawei(config)#vlan 4 smart
     huawei(config)#port vlan 4 0/19 0
     ```

  2. Add a traffic profile.

Copyright © Huawei Technologies Co., Ltd.

```
huawei(config)#traffic table ip index 9 cir off priority 5 priority-policy
local-Setting
```

3. Add a service port to the VLAN.

NOTICE

On the MA5600T/MA5603T/MA5608T, if the PVC is configured with a priority, the priority of the multicast packets carried by the PVC does not take effect.

Add a service port to VLAN 4 and use traffic profile 9.

```
huawei(config)#service-port 100 vlan 4 adsl 0/2/1 vpi 0 vci 35 rx-cttr 9
tx-cttr 9
huawei(config)#service-port 101 vlan 4 adsl 0/3/1 vpi 0 vci 35 rx-cttr 9
tx-cttr 9
```

4. Configure the DHCP relay.

   Configure the IP address of DHCP server 2 and the IP address of the VLAN Layer 3 interface, and bind the VLAN Layer 3 interface to DHCP server 2.

```
huawei(config)#dhcp mode layer-3 standard
huawei(config)#dhcp-server 2 ip 20.2.2.2 20.2.2.3
huawei(config)#interface vlanif 4
huawei(config-if-vlanif4)#ip address 10.2.2.1 24
huawei(config-if-vlanif4)#dhcp-server 2
huawei(config-if-vlanif4)#quit
```

5. Configure the multicast data.

   Configure the multicast mode, authority profile, multicast upstream port, and multicast program. Add multicast user 1 and multicast user 2 to multicast VLAN 4.

```
huawei(config)#multicast-vlan 4
huawei(config-mvlan4)#igmp mode proxy
  Are you sure to change IGMP mode?(y/n)[n]:y
huawei(config-mvlan4)#igmp uplink-port 0/19/0
huawei(config)#btv
huawei(config-btv)#igmp uplink-port-mode default
Are you sure to change the uplink port mode?(y/n)[n]:y
huawei(config)#multicast-vlan 4
huawei(config-mvlan4)#igmp program add name BTV-1 ip 224.1.1.1 sourceip
10.10.10.10
huawei(config-mvlan4)#igmp program add name BTV-2 ip 224.1.1.2 sourceip
10.10.10.10
huawei(config)#btv
huawei(config-btv)#igmp profile profile-name profile0 program-name BTV-1
watch
huawei(config-btv)#igmp policy service-port 100 normal
huawei(config-btv)#igmp policy service-port 101 normal
huawei(config-btv)#igmp user add service-port 100 no-auth
huawei(config-btv)#igmp user add service-port 101 auth
huawei(config-btv)#igmp user bind-profile service-port 101 profile-name
profile0
huawei(config-btv)#quit
huawei(config)#multicast-vlan 4
huawei(config-mvlan4)#igmp multicast-vlan member service-port 100
huawei(config-mvlan4)#igmp multicast-vlan member service-port 101
huawei(config-mvlan4)#quit
```

6. Save the data.

```
huawei(config)#save
```

----End

Copyright © Huawei Technologies Co., Ltd.

Result

After the related upstream device and downstream device are configured, the triple play service (Internet, VoIP, and IPTV services) is available.

- Internet: user 1 and user 2 can access the Internet through PPPoE dialup.
- VoIP: user 1 and user 2 can call each other.
- IPTV: user 1 can watch all the programs after being connected to port 0/2/1, and user 2 can watch only program BTV-1 after being connected to port 0/3/1.

Configuration File

Internet:

```
vlan 2 smart
port vlan 0/19 0
traffic table ip index 7 cir 2048 priority 1 priority-policy local-Setting
service-port vlan 2 adsl 0/2/1 vpi 0 vci 37 rx-cttr 7 tx-cttr 7
service-port vlan 2 adsl 0/3/1 vpi 0 vci 37 rx-cttr 7 tx-cttr 7
dhcp mode layer-3 standard
dhcp-server 1 ip 20.1.1.2 20.1.1 3
save  //Save the configuration.
```

VoIP:

```
vlan 3 smart
port vlan 3 0/19 0
traffic table ip index 8 cir 1024 priority 6 priority-policy local-Setting
service-port vlan 3 adsl 0/2/1 vpi 0 vci 36 rx-cttr 8 tx-cttr 8
service-port vlan 3 adsl 0/3/1 vpi 0 vci 36 rx-cttr 8 tx-cttr 8
dhcp mode layer-3 standard
dhcp-server 1 ip 20.1.1.2 20.1.1 3
interface vlanif 3
ip address 10.1.1.1 24
dhcp-server 1
quit
save  //Save the configuration.
```

IPTV:

```
vlan 4 smart
port vlan 4 0/19 0
traffic table ip index 9 cir off priority 5 priority-policy local-Setting
service-port 100 vlan 4 adsl 0/2/1 vpi 0 vci 35 rx-cttr 9 tx-cttr 9
service-port 101 vlan 4 adsl 0/3/1 vpi 0 vci 35 rx-cttr 9 tx-cttr 9
dhcp mode layer-3 standard
dhcp-server 2 ip 20.2.2.2 20.2.2.3
interface vlanif 4
ip address 10.2.2.1 24
dhcp-server 2
quit
multicast-vlan 4
igmp mode proxy
igmp uplink-port 0/19/0
btv
igmp uplink-port-mode default
quit
multicast-vlan 4
igmp program add name BTV-1 ip 224.1.1.1 sourceip 10.10.10.10
igmp program add name BTV-2 ip 224.1.1.2 sourceip 10.10.10.10
btv
igmp profile profile-name profile0 program-name BTV-1 watch
igmp policy service-port 100 normal
igmp policy service-port 101 normal
```


Copyright © Huawei Technologies Co., Ltd.

```
igmp user add service-port 100 no-auth
igmp user add service-port 101 auth
igmp user bind-profile service-port 101 profile-name profile0
multicast-vlan 4
igmp multicast-vlan member service-port 100
igmp multicast-vlan member service-port 101
quit
save  //Save the configuration.
```

3.4.2 Configuration Example of the Triple Play (Single-PVC for Multiple Services) - Stream-based Rate Limitation

This topic describes how to configure the triple play in the single-PVC for multiple services mode. The user home gateway is connected to multiple terminals to implement the access of multiple services such as Internet access service, VoIP service, and IPTV service.

Prerequisites

- Network devices and lines must be in the normal state.
- The system is working properly.
- The home gateway has been configured. Specifically, virtual local area networks (VLANs) have been configured on the home gateway for different services.
- The asymmetric digital subscriber line 2 plus (ADSL2+) line template and alarm template that need to be bound to ports have been configured. For details about how to configure the ADSL2+ line template or alarm template, see Configuring ADSL2+ Profiles.

Service Requirements

ADSL2+ user 1 and ADSL2+ user 2 are connected to the MA5600T/MA5603T/MA5608T to implement the triple play.

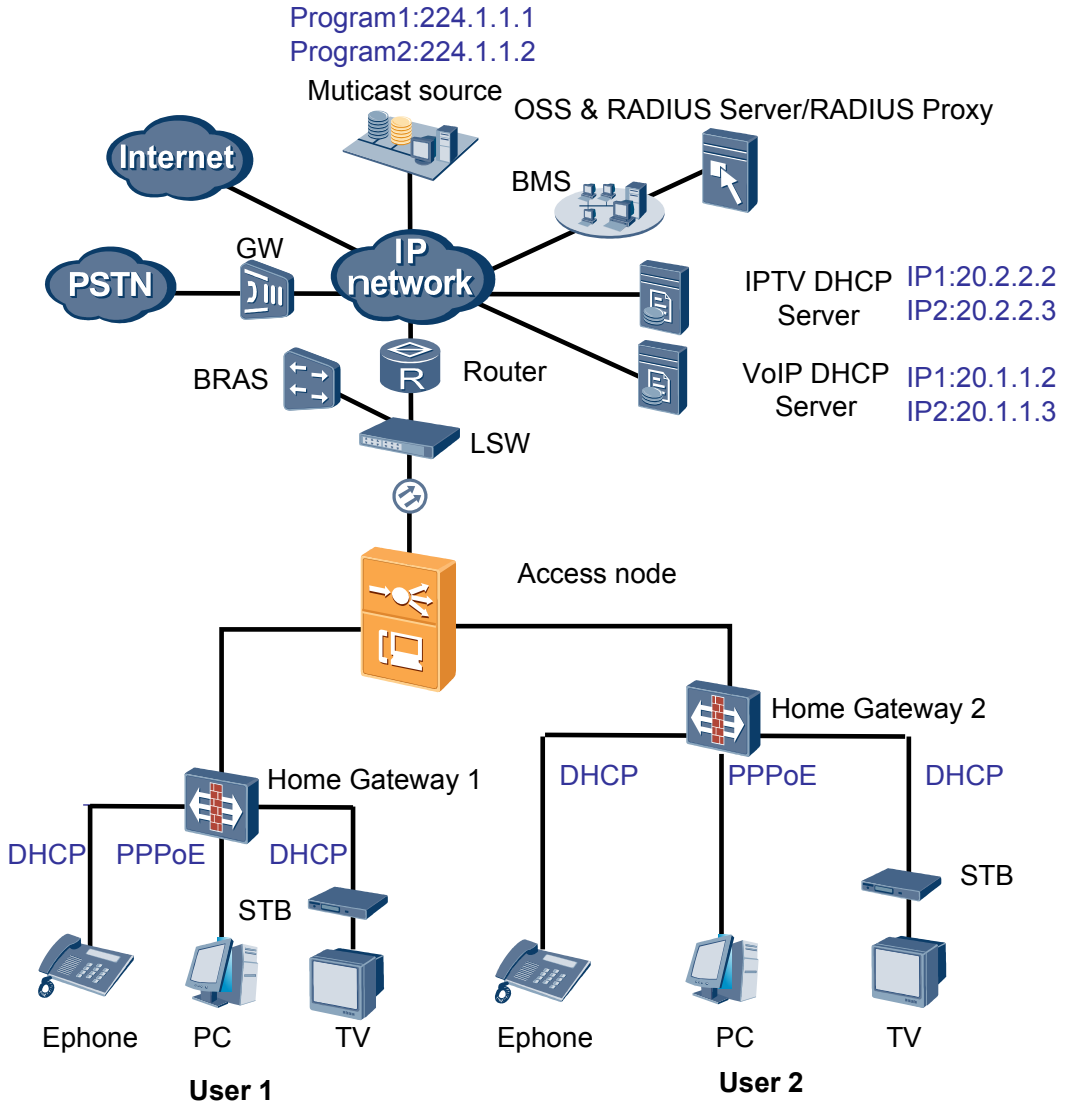
- The PC user accesses the Internet properly.
- The VoIP user makes calls properly.
- The IPTV user watches programs properly.
- After receiving different traffic streams through the same PVC, the MA5600T/MA5603T/MA5608T provides different QoS guarantees to the traffic streams according to the user-side VLANs.

Networking

Figure 3-24 shows an example network of the triple play service in the single-PVC for multiple services mode. The Internet service is accessed in the PPPoE mode. The VoIP service and the IPTV service are provided in the DHCP mode, obtaining IP addresses from the DHCP server in the standard DHCP mode.

Copyright © Huawei Technologies Co., Ltd.

Figure 3-24 Example network of the triple play service in the single-PVC for multiple services mode



Data Plan

Table 3-18 shows the key data for configuring the triple play in single-PVC for multiple services mode on the MA5600T/MA5603T/MA5608T.

Copyright © Huawei Technologies Co., Ltd.

Table 3-18 Data plan for configuring the triple play in single-PVC for multiple services mode (stream-based rate limitation)

Configuration Item	Data			Remarks
	Internet access	VoIP	IPTV	
Upstream port	0/19 0			-
ADSL2+ port	● User 1: 0/2/1 ● User 2: 0/3/1			-
VLAN	● SVLAN ID: 2 ● SVLAN type: smart ● CVLAN ID: 20	● SVLAN ID: 3 ● SVLAN type: smart ● CVLAN ID: 30	● SVLAN ID: 4 ● SVLAN type: smart ● CVLAN ID: 40	-
Traffic profile	● Index: 7 ● CIR: 2 Mbit/s ● Default packet 802.1p priority: 1 ● Priority scheduling policy of downstream packets: Local-Setting	● Index: 8 ● CIR: 1 Mbit/s ● Default packet 802.1p priority: 6 ● Priority scheduling policy of downstream packets: Local-Setting	● Index: 9 ● No rate limitation ● Default packet 802.1p priority: 5 ● Priority scheduling policy of downstream packets: Local-Setting	As VoIP, IPTV, and Internet services access from the same port, the 802.1p priorities for each service must be configured. These three services are prioritized in descending order as follows: VoIP, IPTV, Internet access.
Service port	● VPI: 0 ● VCI: 35	● VPI: 0 ● VCI: 35	● Index: 100 and 101 ● VPI: 0 ● VCI: 35	The three services have different VCIs.

Copyright © Huawei Technologies Co., Ltd.

Configuration Item	Data			Remarks
	Internet access	VoIP	IPTV	
DHCP relay	-	● Number of the DHCP server group: 1 ● IP address of DHCP server group 1: 20.1.1.2 ● IP address of DHCP server group 2: 20.1.1.3 ● IP address of the VLAN Layer 3 interface: 10.1.1.1/24	● Number of the DHCP server group: 2 ● IP address of DHCP server group 1: 20.2.2.2 ● IP address of DHCP server group 2: 20.2.2.3 ● IP address of the VLAN Layer 3 interface: 10.2.2.1/24	-
Multicast	-	-	● Multicast mode: IGMP Proxy ● Profile 0 of multicast user 2: the right to watch only program BTV-1 ● Multicast upstream port: 0/19/0 ● Multicast IP address of program BTV-1: 224.1.1.1; program source IP address: 10.10.10.10 ● Multicast IP address of program BTV-2: 224.1.1.2; program source IP address: 10.10.10.10	-

Copyright © Huawei Technologies Co., Ltd.

Procedure

- Configure the Internet service.
  1. Create a VLAN and add an upstream port to the VLAN.

     ```
     huawei(config)#vlan 2 smart
     huawei(config)#port vlan 2 0/19 0
     ```

  2. Add a traffic profile.

     ```
     huawei(config)#traffic table ip index 7 cir 2048 priority 1 priority-policy local-Setting
     ```

  3. Add a service port to the VLAN.

     Add a service port to VLAN 2 and use the traffic profile added 7 in the preceding step.

     ```
     huawei(config)#service-port vlan 2 adsl 0/2/1 vpi 0 vci 35 multi-service user-vlan 20 rx-cttr 7 tx-cttr 7
     huawei(config)#service-port vlan 2 adsl 0/3/1 vpi 0 vci 35 multi-service user-vlan 20 rx-cttr 7 tx-cttr 7
     ```

  4. Save the data.

     ```
     huawei(config)#save
     ```

- Configure the VoIP service.
  1. Create a VLAN and add an upstream port to the VLAN.

     ```
     huawei(config)#vlan 3 smart
     huawei(config)#port vlan 3 0/19 0
     ```

  2. Add a traffic profile.

     ```
     huawei(config)#traffic table ip index 8 cir 1024 priority 6 priority-policy local-Setting
     ```

  3. Add a service port to the VLAN.

     Add a service port to the VLAN 3 and use the traffic profile 8 added in the preceding step.

     ```
     huawei(config)#service-port vlan 3 adsl 0/2/1 vpi 0 vci 35 multi-service user-vlan 30 rx-cttr 8 tx-cttr 8
     huawei(config)#service-port vlan 3 adsl 0/3/1 vpi 0 vci 35 multi-service user-vlan 30 rx-cttr 8 tx-cttr 8
     ```

     NOTE

     The video and voice services have stricter requirements on delay. You can run the **bind channel** command to bind them to a low delay channel. Currently, this command is available for only the VDSL port.

  4. Configure the DHCP relay.

     Configure the IP addresses of DHCP server 1 and the IP address of the VLAN Layer 3 interface, and bind the VLAN Layer 3 interface to DHCP server 1.

     ```
     huawei(config)#dhcp mode layer-3 standard
     huawei(config)#dhcp-server 1 ip 20.1.1.2 20.1.1 3
     huawei(config)#interface vlanif 3
     huawei(config-if-vlanif3)#ip address 10.1.1.1 24
     huawei(config-if-vlanif3)#dhcp-server 1
     huawei(config-if-vlanif3)#quit
     ```

  5. Save the data.

     ```
     huawei(config)#save
     ```

- Configure the IPTV service.
  1. Create a VLAN and add an upstream port to the VLAN.

     ```
     huawei(config)#vlan 4 smart
     ```


Copyright © Huawei Technologies Co., Ltd.

```
huawei(config)#port vlan 4 0/19 0
```

2. Add a traffic profile.

```
huawei(config)#traffic table ip index 9 cir off priority 5 priority-policy
local-Setting
```

3. Add a service port to the VLAN.

NOTICE

On the MA5600T/MA5603T/MA5608T, if the PVC is configured with a priority, the priority of the multicast packets carried by the PVC does not take effect.

Add a service port to VLAN 4 and use traffic profile 9.

```
huawei(config)#service-port 100 vlan 4 adsl 0/2/1 vpi 0 vci 35 multi-
service user-vlan 40 rx-cttr 9 tx-cttr 9
huawei(config)#service-port 101 vlan 4 adsl 0/3/1 vpi 0 vci 35 multi-
service user-vlan 40 rx-cttr 9 tx-cttr 9
```

4. Configure the DHCP relay.

   Configure the IP addresses of DHCP server 2 and the IP address of the VLAN Layer 3 interface, and bind the VLAN Layer 3 interface to DHCP server 2.

```
huawei(config)#dhcp mode layer-3 standard
huawei(config)#dhcp-server 2 ip 20.2.2.2 20.2.2.3
huawei(config)#interface vlanif 4
huawei(config-if-vlanif4)#ip address 10.2.2.1 24
huawei(config-if-vlanif4)#dhcp-server 2
huawei(config-if-vlanif4)#quit
```

5. Configure the multicast data.

   Configure the multicast mode, authority profile, multicast upstream port, and multicast program. Add multicast user 1 and multicast user 2 to multicast VLAN 4.

```
huawei(config)#multicast-vlan 4
huawei(config-mvlan4)#igmp mode proxy
  Are you sure to change IGMP mode?(y/n)[n]:y
huawei(config-mvlan4)#igmp uplink-port 0/19/0
huawei(config)#btv
huawei(config-btv)#igmp uplink-port-mode default
Are you sure to change the uplink port mode?(y/n)[n]:y
huawei(config)#multicast-vlan 4
huawei(config-mvlan4)#igmp program add name BTV-1 ip 224.1.1.1 sourceip
10.10.10.10
huawei(config-mvlan4)#igmp program add name BTV-2 ip 224.1.1.2 sourceip
10.10.10.10
huawei(config)#btv
huawei(config-btv)#igmp profile profile-name profile0 program-name BTV-1
watch
huawei(config-btv)#igmp policy service-port 100 normal
huawei(config-btv)#igmp policy service-port 101 normal
huawei(config-btv)#igmp user add service-port 100 no-auth
huawei(config-btv)#igmp user add service-port 101 auth
huawei(config-btv)#igmp user bind-profile service-port 101 profile-name
profile0
huawei(config)#multicast-vlan 4
huawei(config-mvlan4)#igmp multicast-vlan member port 0/2/1
huawei(config-mvlan4)#igmp multicast-vlan member port 0/3/1
huawei(config-mvlan4)#quit
```

6. Save the data.

Copyright © Huawei Technologies Co., Ltd.

```
huawei(config)#save
```

----End

Result

After the related upstream device and downstream device are configured, the triple play service (Internet, VoIP, and IPTV services) is available.

- Internet: user 1 and user 2 can access the Internet through PPPoE dialup.
- VoIP: user 1 and user 2 can call each other.
- IPTV: user 1 can watch all the programs after being connected to port 0/2/1, and user 2 can watch only program BTV-1 after being connected to port 0/3/1.

Configuration File

Internet:

```
vlan 2 smart
port vlan 0/19 0
traffic table ip index 7 cir 2048 priority 1 priority-policy local-Setting
service-port vlan 2 adsl 0/2/1 vpi 0 vci 35 multi-service user-vlan 20 rx-cttr 7 tx-
cttr 7
service-port vlan 2 adsl 0/3/1 vpi 0 vci 35 multi-service user-vlan 20 rx-cttr 7 tx-
cttr 7
dhcp mode layer-3 standard
dhcp-server 1 ip 20.1.1.2 20.1.1 3
save
```

VoIP:

```
vlan 3 smart
port vlan 3 0/19 0
traffic table ip index 8 cir 1024 priority 6 priority-policy local-Setting
service-port vlan 3 adsl 0/2/1 vpi 0 vci 35 multi-service user-vlan 30 rx-cttr 8 tx-
cttr 8
service-port vlan 3 adsl 0/3/1 vpi 0 vci 35 multi-service user-vlan 30 rx-cttr 8 tx-
cttr 8
dhcp mode layer-3 standard
dhcp-server 1 ip 20.1.1.2 20.1.1 3
interface vlanif 3
ip address 10.1.1.1 24
dhcp-server 1
quit
save
```

IPTV:

```
vlan 4 smart
port vlan 4 0/19 0
traffic table ip index 9 cir off priority 5 priority-policy local-Setting
service-port 100 vlan 4 adsl 0/2/1 vpi 0 vci 35 multi-service user-vlan 40 rx-cttr
9 tx-cttr 9
service-port 101 vlan 4 adsl 0/3/1 vpi 0 vci 35 multi-service user-vlan 40 rx-cttr
9 tx-cttr 9
dhcp mode layer-3 standard
dhcp-server 2 ip 20.2.2.2 20.2.2.3
interface vlanif 4
ip address 10.2.2.1 24
dhcp-server 2
quit
multicast-vlan 4
igmp mode proxy
```


Copyright © Huawei Technologies Co., Ltd.

```
igmp uplink-port 0/19/0
btv
igmp uplink-port-mode default
multicast-vlan 4
igmp program add name BTV-1 ip 224.1.1.1 sourceip 10.10.10.10
igmp program add name BTV-2 ip 224.1.1.2 sourceip 10.10.10.10
btv
igmp profile profile-name profile0 program-name BTV-1 watch
igmp policy service-port 100 normal
igmp policy service-port 101 normal
igmp user add service-port 100 no-auth
igmp user add service-port 101 auth
igmp user bind-profile service-port 101 profile-name profile0
multicast-vlan 4
igmp multicast-vlan member service-port 100
igmp multicast-vlan member service-port 101
quit
save
```

3.4.3 Configuration Example of the Triple Play Service (Single-PVC for Multiple Services) - User-based and Stream-based Rate Limitation

This topic describes how to configure the triple play service in the single-PVC for multiple services mode. The user home gateway is connected to multiple terminals to implement the access of multiple services such as Internet access, VoIP, and IPTV services and perform user-based and stream-based rate limitation.

Prerequisites

- Network devices and lines must be in the normal state.
- The system is working properly.
- The home gateway has been configured. Specifically, virtual local area networks (VLANs) have been configured on the home gateway for different services.
- The asymmetric digital subscriber line 2 plus (ADSL2+) line template and alarm template that need to be bound to ports have been configured.

Service Requirements

ADSL2+ user 1 and ADSL2+ user 2 are connected to the MA5600T/MA5603T/MA5608T to implement the triple play.

- The PC user accesses the Internet properly.
- The VoIP user makes calls properly.
- The IPTV user watches programs properly.
- The maximum bandwidth of each user is 10 Mbit/s, adopting user-based bandwidth management: The Internet access, VoIP, and IPTV services of each user share the same total bandwidth and the QoS scheduling is implemented. The service priorities are VoIP (the value is 6), IPTV (the value is 5), and Internet access (the value is 1) in descending order. If any two services carry no traffic, the third service can hold a burst of the total user bandwidth.

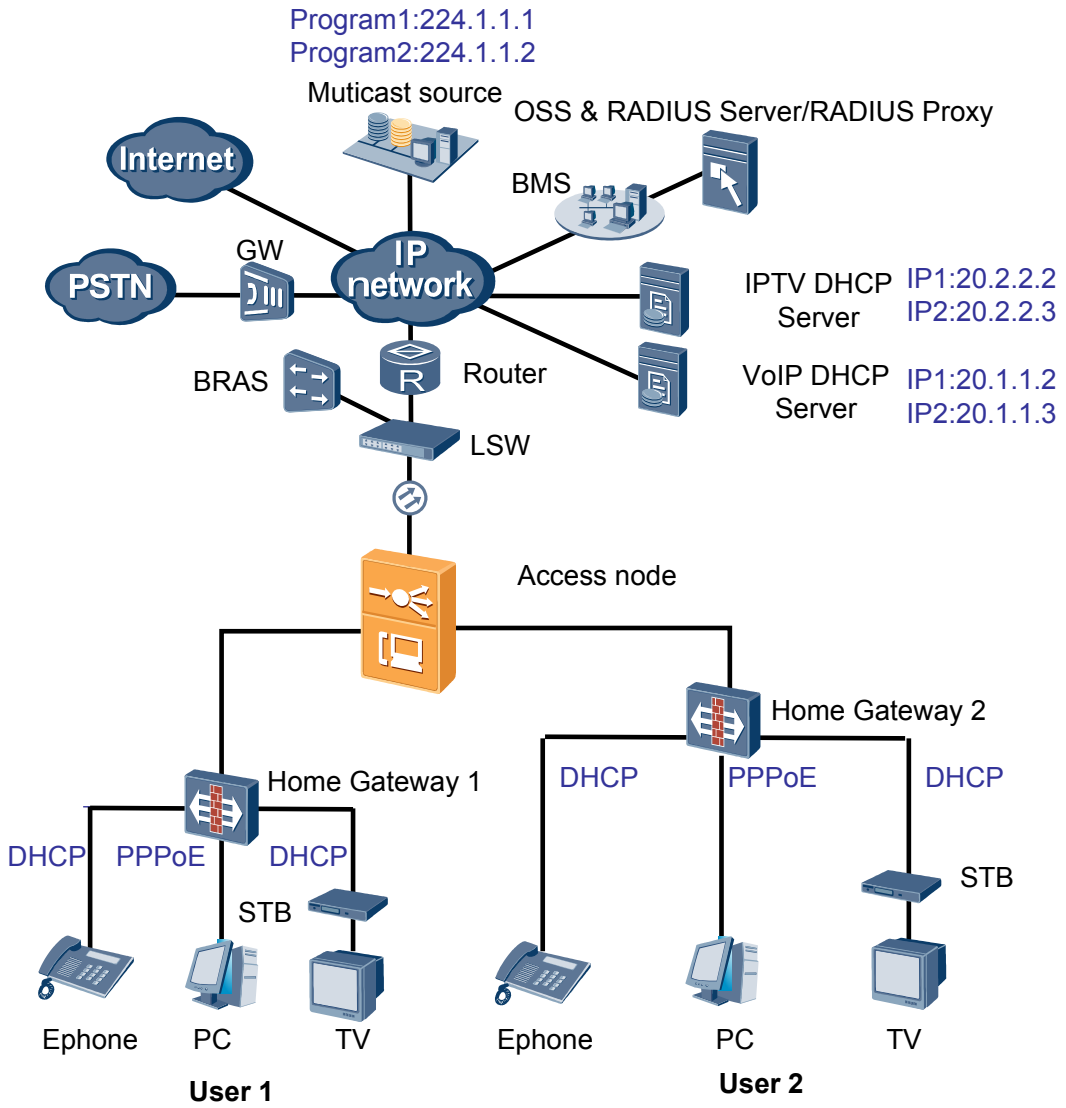
Copyright © Huawei Technologies Co., Ltd.

- After receiving different traffic streams through the same PVC, the MA5600T/MA5603T/MA5608T provides different QoS guarantees to the traffic streams according to the user-side VLANs.

Networking

Figure 3-25 shows an example network of the triple play in the single PVC for multiple services mode. The Internet service is accessed in the PPPoE mode. The VoIP service and the IPTV service are provided in the DHCP mode, obtaining IP addresses from the DHCP server in the standard DHCP mode.

Figure 3-25 Example network of the triple play service in the single-PVC for multiple services mode



Copyright © Huawei Technologies Co., Ltd.

Data Plan

Table 3-19 shows the key data for configuring the triple play in single-PVC for multiple services mode on the MA5600T/MA5603T/MA5608T.

Table 3-19 Data plan for configuring the triple play in single-PVC for multiple services mode (user-based and stream-based rate limitation)

Configuration Item	Data			Remarks
	Internet access	VoIP	IPTV	
Upstream port	0/19 0			-
ADSL2+ port	● User 1: 0/2/0 ● User 2: 0/2/1 ● ADSL2+ channel profile – ID: 3 – Minimum upstream/downstream rates: 32 kbit/s – Minimum reserved upstream/downstream rate: 32 kbit/s – Maximum upstream rate: 4096 kbit/s – Maximum downstream rate: 10240 kbit/s ● ADSL2+ line template: – ID: 3 – Upstream/Downstream rate adaptation ratio of channel: 100 ● ADSL2+ line alarm template ID: 1			-
VLAN	● SVLAN ID: 2 ● SVLAN type: smart ● CVLAN ID: 20	● SVLAN ID: 3 ● SVLAN type: smart ● CVLAN ID: 30	● SVLAN ID: 4 ● SVLAN type: smart ● CVLAN ID: 40	-

Copyright © Huawei Technologies Co., Ltd.

Configuration Item	Data			Remarks
	Internet access	VoIP	IPTV	
Traffic profile	● Index: 7 ● CIR: 2 Mbit/s ● PIR: 10 Mbit/s ● Default packet 802.1p priority: 1 ● Priority scheduling policy of downstream packets: Local-Setting	● Index: 8 ● CIR: 1 Mbit/s ● PIR: 10 Mbit/s ● Default packet 802.1p priority: 6 ● Priority scheduling policy of downstream packets: Local-Setting	● Index: 9 ● CIR: 4 Mbit/s ● PIR: 10 Mbit/s ● Default packet 802.1p priority: 5 ● Priority scheduling policy of downstream packets: Local-Setting	As VoIP, IPTV, and Internet services access from the same port, the 802.1p priorities for each service must be configured. These three services are prioritized in descending order as follows: VoIP, IPTV, Internet access. The PIR and maximum user bandwidth must be the same.
Service port	● VPI: 0 ● VCI: 35	● VPI: 0 ● VCI: 35	● Index: 100 and 101 ● VPI: 0 ● VCI: 35	The three services have different VCIs.
DHCP relay	-	● Number of the DHCP server group: 1 ● IP address of DHCP server group 1: 20.1.1.2 ● IP address of DHCP server group 2: 20.1.1.3 ● IP address of the VLAN Layer 3 interface: 10.1.1.1/24	● Number of the DHCP server group: 2 ● IP address of DHCP server group 1: 20.2.2.2 ● IP address of DHCP server group 2: 20.2.2.3 ● IP address of the VLAN Layer 3 interface: 10.2.2.1/24	-

Copyright © Huawei Technologies Co., Ltd.

Configuration Item	Data			Remarks
	Internet access	VoIP	IPTV	
Multicast	-	-	● Multicast mode: IGMP Proxy ● Profile 0 of multicast user 2: the right to watch only program BTV-1 ● Multicast upstream port: 0/19/0 ● Multicast IP address of program BTV-1: 224.1.1.1; program source IP address: 10.10.10.10 ● Multicast IP address of program BTV-2: 224.1.1.2; program source IP address: 10.10.10.10	-

Procedure

- Configure user bandwidth management.
  1. Configure ADSL channel profile 3 with a minimum upstream/downstream transmission rate 32 kbit/s, a minimum upstream/downstream reserved rate 32 kbit/s, a maximum downstream transmission rate 10240 kbit/s and a maximum upstream transmission rate 4096 kbit/s.

     ```
     huawei(config)#adsl channel-profile quickadd 3 rate 32 32 10240 32 32 4096
     ```

  2. Configure ADSL line template 3 by binding channel profile 3.

     ```
     huawei(config)#adsl line-template quickadd 3 channel1 3 100 100
     ```

- Bind ADSL line template 3 created in the previous step to ADSL ports 0/2/0 and 0/2/1. Activate the ports.

```
huawei(config)#interface adsl 0/2
huawei(config-if-adsl-0/2)#deactivate 0
huawei(config-if-adsl-0/2)#deactivate 1
huawei(config-if-adsl-0/2)#activate 0 template-index 3
huawei(config-if-adsl-0/2)#activate 1 template-index 3
huawei(config-if-adsl-0/2)#alarm-config 0 1
```


Copyright © Huawei Technologies Co., Ltd.

```
huawei(config-if-adsl-0/2)#alarm-config 1 1
huawei(config-if-adsl-0/2)#quit
```

- Configure the queue scheduling mode of the port.

  Configure the queue scheduling mode of the port to priority queuing (PQ).

  ```
  huawei(config)#queue-scheduler strict-priority
  ```

- Configure the Internet access service.

  1. Create a VLAN and add an upstream port to the VLAN.

     ```
     huawei(config)#vlan 2 smart
     huawei(config)#port vlan 2 0/19 0
     ```

  2. Configure a traffic profile.

     ```
     huawei(config)#traffic table ip index 7 cir 2048 pir 10240 priority 1
     priority-
     policy local-Setting
     ```

  3. Add a service port to the VLAN.

     Create service virtual port, the S-VLAN ID to 2, the C-VLAN ID to 20, the VPI/VCI to 0/35 and use the traffic profile 7 added in the preceding step.

     ```
     huawei(config)#service-port vlan 2 adsl 0/2/0 vpi 0 vci 35
     multi-service user-vlan 20 rx-cttr 7 tx-cttr 7
     huawei(config)#service-port vlan 2 adsl 0/2/1 vpi 0 vci 35
     multi-service user-vlan 20 rx-cttr 7 tx-cttr 7
     ```

  4. Save the data.

     ```
     huawei(config)#save
     ```

- Configure the VoIP service.

  1. Create a VLAN and add an upstream port to the VLAN.

     ```
     huawei(config)#vlan 3 smart
     huawei(config)#port vlan 3 0/19 0
     ```

  2. Configure a traffic profile.

     ```
     huawei(config)#traffic table ip index 8 cir 1024 pir 10240 priority 6
     priority-policy local-Setting
     ```

  3. Add a service port to the VLAN.

     Create service virtual port, the S-VLAN ID to 3, the C-VLAN ID to 30, the VPI/VCI to 0/35 and use the traffic profile 8added in the preceding step.

     ```
     huawei(config)#service-port vlan 3 adsl 0/2/0 vpi 0 vci 35
     multi-service user-vlan 30 rx-cttr 8 tx-cttr 8
     huawei(config)#service-port vlan 3 adsl 0/2/1 vpi 0 vci 35
     multi-service user-vlan 30 rx-cttr 8 tx-cttr 8
     ```

     NOTE

     The video and voice services have stricter requirements on delay. You can run the **bind channel** command to bind them to a low delay channel. Currently, this command is available for only the VDSL2 port.

  4. Configure the DHCP relay.

     Configure the IP addresses of DHCP server 1 and the IP address of the VLAN Layer 3 interface, and bind the VLAN Layer 3 interface to DHCP server 1.

     ```
     huawei(config)#dhcp mode layer-3 standard
     huawei(config)#dhcp-server 1 ip 20.1.1.2 20.1.1 3
     huawei(config)#interface vlanif 3
     huawei(config-if-vlanif3)#ip address 10.1.1.1 24
     huawei(config-if-vlanif3)#dhcp-server 1
     huawei(config-if-vlanif3)#quit
     ```


Copyright © Huawei Technologies Co., Ltd.

5. Save the data.

```
huawei(config)#save
```

- Configure the IPTV service.

1. Create a VLAN and add an upstream port to the VLAN.

```
huawei(config)#vlan 4 smart
huawei(config)#port vlan 4 0/19 0
```

2. Configure a traffic profile.

```
huawei(config)#traffic table ip index 9 cir 4096 pir 10240 priority 5
priority-policy local-Setting
```

3. Add a service port to the VLAN.

NOTICE

On the MA5600T/MA5603T/MA5608T, if the PVC is configured with a priority, the priority of the multicast packets carried by the PVC does not take effect.

Create service virtual port, and use the traffic profile 9 added in the preceding step.

```
huawei(config)#service-port 100 vlan 4 adsl 0/2/0 vpi 0 vci 35
multi-service user-vlan 40 rx-cttr 9 tx-cttr 9
huawei(config)#service-port 101 vlan 4 adsl 0/2/1 vpi 0 vci 35
multi-service user-vlan 40 rx-cttr 9 tx-cttr 9
```

4. Configure the DHCP relay.

Configure the IP addresses of DHCP server 2 and the IP address of the VLAN Layer 3 interface, and bind the VLAN Layer 3 interface to DHCP server 2.

```
huawei(config)#dhcp mode layer-3 standard
huawei(config)#dhcp-server 2 ip 20.2.2.2 20.2.2.3
huawei(config)#interface vlanif 4
huawei(config-if-vlanif4)#ip address 10.2.2.1 24
huawei(config-if-vlanif4)#dhcp-server 2
huawei(config-if-vlanif4)#quit
```

5. Configure the multicast data.

Configure the multicast mode, authority profile, multicast upstream port, and multicast program. Add multicast user 1 and multicast user 2 to multicast VLAN 4.

```
huawei(config)#multicast-vlan 4
huawei(config-mvlan4)#igmp mode proxy
  Are you sure to change IGMP mode?(y/n)[n]:y
huawei(config-mvlan4)#igmp uplink-port 0/19/0
huawei(config-mvlan4)#btv
huawei(config-btv)#igmp uplink-port-mode default
Are you sure to change the uplink port mode?(y/n)[n]:y
huawei(config-btv)#quit
huawei(config)#multicast-vlan 4
huawei(config-mvlan4)#igmp program add name BTV-1 ip 224.1.1.1 sourceip
10.10.10.10
huawei(config-mvlan4)#igmp program add name BTV-2 ip 224.1.1.2 sourceip
10.10.10.10
huawei(config-mvlan4)#btv
huawei(config-btv)#igmp profile profile-name profile0 program-name BTV-1
watch
huawei(config-btv)#igmp policy service-port 100 normal
huawei(config-btv)#igmp policy service-port 101 normal
huawei(config-btv)#igmp user add port service-port 100 auth
huawei(config-btv)#igmp user add port service-port 101 auth
huawei(config-btv)#igmp user bind-profile service-port 100 profile-name
```


Copyright © Huawei Technologies Co., Ltd.

```
profile0
huawei(config-btv)#multicast-vlan 4
huawei(config-mvlan4)#igmp multicast-vlan member service-port 100
huawei(config-mvlan4)#igmp multicast-vlan member service-port 101
huawei(config-mvlan4)#quit
```

6. Save the data.

```
huawei(config)#save
```

----End

Result

After the relevant upstream device and downstream device are configured, the triple play service (Internet access, VoIP, and IPTV services) is available. If any two services carry no traffic, the third service can hold a burst of the total user bandwidth.

- Internet: user 1 and user 2 can access the Internet through PPPoE dialup.
- VoIP: user 1 and user 2 can call each other.
- IPTV: user 1 can watch all the programs after being connected to port 0/2/0, and user 2 can watch only program BTV-1 after being connected to port 0/2/1.

Configuration File

```
adsl channel-profile quickadd 3 rate 32 32 10240 32 32 4096
adsl line-template quickadd 3 channel1 3 100 100
queue-scheduler strict-priority
interface adsl 0/2
deactivate 0
deactivate 1
activate 0 template-index 3
activate 1 template-index 3
alarm-config 0 1
alarm-config 1 1
quit
```

Internet:

```
vlan 2 smart
port vlan 0/19 0
traffic table ip index 7 cir 10240 priority 1 priority-policy local-Setting
service-port vlan 2 adsl 0/2/0
vpi 0 vci 35 multi-service user-vlan 20 rx-cttr 7 tx-cttr 7
service-port vlan 2 adsl 0/2/1
vpi 0 vci 35 multi-service user-vlan 20 rx-cttr 7 tx-cttr 7
dhcp mode layer-3 standard
dhcp-server 1 ip 20.1.1.2 20.1.1 3
save
```

VoIP:

```
vlan 3 smart
port vlan 3 0/19 0
traffic table ip index 8 cir 10240 priority 6 priority-policy local-Setting
service-port vlan 3 adsl 0/2/0
vpi 0 vci 35 multi-service user-vlan 30 rx-cttr 8 tx-cttr 8
service-port vlan 3 adsl 0/2/1
vpi 0 vci 35 multi-service user-vlan 30 rx-cttr 8 tx-cttr 8
dhcp mode layer-3 standard
dhcp-server 1 ip 20.1.1.2 20.1.1 3
interface vlanif 3
ip address 10.1.1.1 24
dhcp-server 1
```


Copyright © Huawei Technologies Co., Ltd.

```
quit
save
```

IPTV:

```
vlan 4 smart
port vlan 4 0/19 0
traffic table ip index 9 cir off priority 5 priority-policy local-Setting
service-port 100 vlan 4 adsl  0/2/0
vpi 0 vci 35 multi-service user-vlan 40 rx-cttr 9 tx-cttr 9
service-port 101 vlan 4 adsl 0/2/1
 vpi 0 vci 35 multi-service user-vlan 40 rx-cttr 9 tx-cttr 9
dhcp mode layer-3 standard
dhcp-server 2 ip 20.2.2.2 20.2.2.3
interface vlanif 4
ip address 10.2.2.1 24
dhcp-server 2
quit
multicast-vlan 4
igmp mode proxy
igmp uplink-port 0/19/0
btv
igmp uplink-port-mode default
quit
multicast-vlan 4
igmp program add name BTV-1 ip 224.1.1.1 sourceip 10.10.10.10
igmp program add name BTV-2 ip 224.1.1.2 sourceip 10.10.10.10
btv
igmp profile profile-name profile0 program-name BTV-1 watch
igmp policy service-port 100 normal
igmp policy service-port 101 normal
igmp user add service-port 100 no-auth
igmp user add service-port 101 auth
igmp user bind-profile service-port 100 profile-name profile0
multicast-vlan 4
igmp multicast-vlan member service-port 100
igmp multicast-vlan member service-port 101
quit
save
```


Copyright © Huawei Technologies Co., Ltd.

4 Configuration Example of the Private Line Service

About This Chapter

A private line service refers to a service carried over a true or virtual private line on the public network for transparent transmission and for access of private network services. This topic describes how to configure the private line service.

Context

The MA5600T/MA5603T/MA5608T supports the following private line services:

- PWE3 private line service
- TDM SHDSL access service
- QinQ VLAN private line service

4.1 Example: Configuring the QinQ VLAN
The QinQ-VLAN-based private line service can achieve the interconnection and secure communication among branches in different areas within the enterprise private network.

4.2 Example: Configuring VLAN Stacking Multi-ISP Wholesale Access
In a Layer-2 switching metropolitan area network (MAN), there are multiple Internet service providers (ISPs). To provision the services provided by the ISP to the specified user group rapidly, the outer VLAN tags of VLAN stacking can be used to identify ISPs, while the inner VLAN tags to identify users. In this way, different user groups can be connected to the specified ISPs in batches through different outer VLAN tags to obtain services from the ISPs.

4.3 Configuration Example of the PWE3 Private Line Service
This topic describes how to configure the MPLS PWE3 private line service using examples.

4.4 Configuration Example of TDM SHDSL for Transparently Transmitting the Narrowband Data Private Line Service
The TDM SHDSL extends the access distance. With the TDM SHDSL, the MA5600T/MA5603T/MA5608T transparently transmits user-side configuration data to the digital data network (DDN). In this way, the twisted pair can be fully used and the E1 line deployment expense decreases.

Copyright © Huawei Technologies Co., Ltd.

4.5 Configuration Example of the Private Line Service Leasing E1 Timeslots

Leasing an entire E1 line is expensive and also a waste of the bandwidth resources. The private line service leasing E1 timeslots can meet the requirement leasing a part of an E1 line. With this service, users are assigned specific timeslots of an E1 line, and therefore can share the bandwidth of the E1 line, hence saving the E1 line lease expense.

Copyright © Huawei Technologies Co., Ltd.

4.1 Example: Configuring the QinQ VLAN

The QinQ-VLAN-based private line service can achieve the interconnection and secure communication among branches in different areas within the enterprise private network.

Prerequisites

- Network devices and lines must be in the normal state.
- The authentication data of the access user must be configured on the BRAS.
- The system is working properly.

Service Requirements

- An enterprise requires to achieve the interconnection and secure communication between its headquarters and the branches located in different areas through Layer 2 switching network, and to isolate the data of different departments.
- The access device uses xDSL or LAN access.

Networking

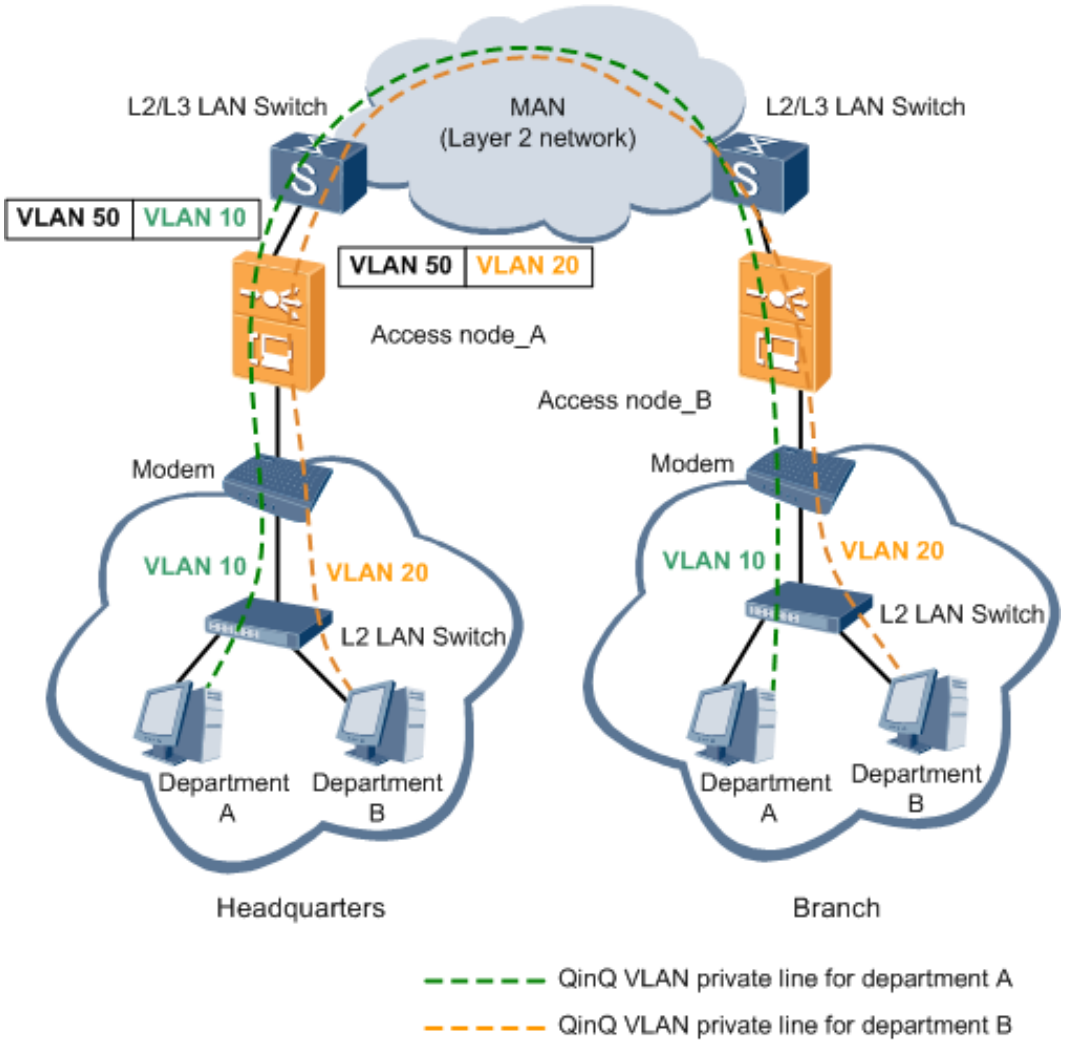
Figure 4-1 shows an example network for configuring the private line service.

The two branches of the enterprise are connected to the (metropolitan area network) MAN through the MA5600T/MA5603T/MA5608T. The upper-layer network must work in the Layer 2 mode, and must forward packets according to the VLAN and the MAC address.

On the MA5600T/MA5603T/MA5608T, the attribute of the upstream VLAN of user packets is configured as QinQ private line service. A VLAN tunnel is created in Layer 2/Layer 3 MAN for transmitting data carrying the VLAN tag. Different VLAN IDs are used for different departments to achieve user isolation and data security. In this way, the service packets of the enterprise private network can be transparently transmitted through the public network, and the two branches can communicate with each other securely.

Copyright © Huawei Technologies Co., Ltd.

Figure 4-1 Example network for configuring the private line service



The configuration on MA5600T/MA5603T/MA5608T_A is the same as the configuration on MA5600T/MA5603T/MA5608T_B. The following uses the configuration on MA5600T/MA5603T/MA5608T_A and VDSL2 access as examples to describe how to configure the private line service implemented through a QinQ VLAN.

Data Plan

Table 4-1 lists the key data planning of the QinQ VLAN private line service on MA5600T/MA5603T/MA5608T_A.

Copyright © Huawei Technologies Co., Ltd.

Table 4-1 Data plan for configuring the QinQ VLAN private line service

Item	Data	Remarks
VLAN	● VLAN ID: 50 ● VLAN type: smart VLAN ● VLAN attribute: QinQ	The public network VLAN, namely outer VLAN, is configured here. The inner VLAN belongs to the enterprise private network, which can be planned by the enterprise self.
Transparent transmission of Layer 2 packets	Enable the transparent transmission of BPDUs.	This function is mainly used in the QinQ service to provide a transparent and secure data channel for the enterprise branches located in two places within the enterprise private network. After the transparent transmission of BPDUs is enabled, the Layer 2 protocol packets of a private network can be transparently transmitted through the public network.
Upstream port	0/19/0	-
Traffic profile	● Traffic profile ID: 10 ● CIR: 4 Mbit/s ● Priority copy policy: user-cos ● Default 802.1p priority of the packet: 4 ● Priority-based scheduling policy of the downstream packets: local-setting	The CIR depends on the user bandwidth requirement.
VDSL2 port	● VDSL2 port ID: 0/2/0 ● Default VDSL2 line profile: 1 ● Default VDSL2 alarm profile: 1	-
Service virtual port	● VLAN ID: 50 ● Service port: 0/2/0 ● VDSL channel mode: ATM ● VPI: 0 ● VCI: 35 ● ID of the traffic profile in Rx direction: 10 ● ID of the traffic profile in Tx direction: 10	● The VPI/VCI is the same as the management VPI/VCI on the peer modem. ● The traffic profile that meets the service requirement is used.

Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Create a VLAN.

The VLAN ID is 50, and the VLAN is a smart VLAN.

```
huawei(config)#vlan 50 smart
```

Step 2 Set the VLAN attribute to QinQ.

```
huawei(config)#vlan attrib 50 q-in-q
```

Step 3 Enable the transparent transmission of BPDUs.

Enable the transparent transmission of BPDUs so that the Layer 2 protocol packets of a private network can be transparently transmitted through the public network. By default, the transparent transmission of BPDUs is disabled.

```
huawei(config)#bpdu tunnel vlan 50 enable
```

Step 4 Add an upstream port to the VLAN.

Add upstream port 0/19/0 to VLAN 50.

```
huawei(config)#port vlan 50 0/19 0
```

Step 5 Add a traffic profile.

The profile ID is 10, the CIR is 4 Mbit/s, and packets are scheduled according to the priority specified in the traffic profile.

```
huawei(config)#traffic table ip index 10 cir 4096 priority user-cos 4 priority-policy
 local-Setting
```

Step 6 Activate the VDSL2 port and bind a profile to it.

Use the default VDSL2 line profile 1. Activate port 0/2/0 and bind alarm profile 1 to port 0/2/0.

NOTE

- By default, the VDSL port is in the activated state. Before binding a profile to the port, you must deactivate the port.

```
huawei(config)#interface vdsl 0/2
huawei(config-if-vdsl-0/2)#deactivate 0
huawei(config-if-vdsl-0/2)#activate 0 template-index 1
huawei(config-if-vdsl-0/2)#alarm-config 0 1
huawei(config-if-vdsl-0/2)#quit
```

Step 7 Add a service port to the VLAN.

Add a service port to the VLAN 50, and use traffic profile 10 that meets the service requirements. The VPI and the VCI are 0 and 35 respectively, the same as those on the peer modem. The user port is 0/2/0. The VDSL channel is in ATM mode.

```
huawei(config)#service-port vlan 50 vdsl mode atm 0/2/0 vpi 0 vci 35 rx-cttr 10 tx-cttr 10
```

Step 8 Save the data.

```
huawei(config)#save
```

----End

Copyright © Huawei Technologies Co., Ltd.

Result

After the configuration, the two branches of the enterprise can communicate with each other.

Configuration File

```
vlan 50 smart
vlan attrib 50 q-in-q
port vlan 50 0/19 0
bpdu tunnel vlan 50 enable
traffic table ip index 10 cir 4096 priority user-cos 4 priority-policy local-
Setting
interface vdsl 0/2
deactivate 0
activate 0 template-index 1
alarm-config 0 1
quit
service-port vlan 50 vdsl mode atm 0/2/0 vpi 0 vci 35 rx-cttr 10 tx-cttr 10
save
```

4.2 Example: Configuring VLAN Stacking Multi-ISP Wholesale Access

In a Layer-2 switching metropolitan area network (MAN), there are multiple Internet service providers (ISPs). To provision the services provided by the ISP to the specified user group rapidly, the outer VLAN tags of VLAN stacking can be used to identify ISPs, while the inner VLAN tags to identify users. In this way, different user groups can be connected to the specified ISPs in batches through different outer VLAN tags to obtain services from the ISPs.

Prerequisites

- Network devices and lines must be in the normal state.
- The authentication data of the access user must be configured on the BRAS.
- The system is working properly.

Service Requirements

- The two ISPs in the Layer-2 switching MAN provide broadband services to enterprise users. Different enterprise user groups are bulk connected to the specified ISP to obtain services provided by the ISP.
- The access device uses xDSL or LAN access.

Networking

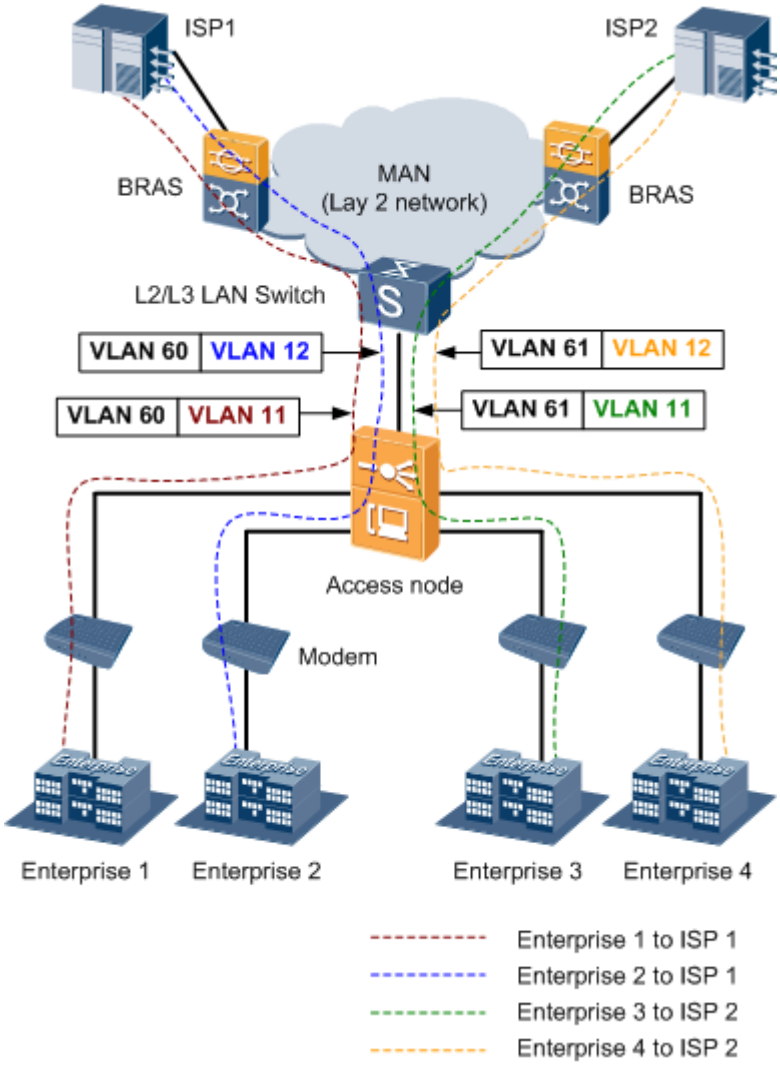
Figure 4-2 shows an example network for configuring the VLAN stacking multi-ISP wholesale access.

Enterprise 1 and 2 belong to ISP 1, and enterprise 3 and 4 belong to ISP 2. Based on the VLAN stacking feature. The upper-layer network must work in the Layer 2 mode, and must forward packets according to the VLAN and the MAC address. The MA5600T/MA5603T/MA5608T adds the outer VLAN tag to differentiate ISPs and inner VLAN tag to differentiate users and forwards the user packet to the Layer 2 network. Then the Layer 2/Layer 3 LAN switch forwards the user packets to the specified ISP BRAS based on the outer VLAN tag. The ISP BRAS

Copyright © Huawei Technologies Co., Ltd.

removes the outer VLAN tag and identify the users based on the inner VLAN tag. After passing the authentication, the enterprise users can obtain various services provided by the ISP.

Figure 4-2 Example network for configuring the VLAN stacking multi-ISP wholesale access



Data Plan

Table 4-2 lists the key data planning of the VLAN stacking wholesale service on the MA5600T/MA5603T/MA5608T. The ADSL2+ access is used as an example.

Copyright © Huawei Technologies Co., Ltd.

Table 4-2 Data plan for configuring the VLAN stacking wholesale service

Item	Data	Remarks
VLAN	VLAN ID: ● ISP1: 60 – Enterprise user 1: 11 – Enterprise user 2: 12 ● ISP2: 61 – Enterprise user 3: 11 – Enterprise user 4: 12 ● VLAN type: smart VLAN ● VLAN attribute: stacking	The outer VLAN identifies the ISP, and inner VLAN identifies the user. The inner VLAN tags must be unique under the same ISP, but can be the same under different ISPs.
Upstream port	0/19/0	-
Traffic profile	● Traffic profile ID: 10 ● CIR: 2 Mbit/s ● Priority copy policy: user-cos ● Default 802.1p priority of the packet: 4 ● Priority-based scheduling policy of the downstream packets: local-setting	The CIR depends on the user bandwidth requirement.
ADSL2+ port	● ADSL2+ port ID – Enterprise user 1: 0/2/0 – Enterprise user 2: 0/2/1 – Enterprise user 3: 0/3/0 – Enterprise user 4: 0/3/1 ● Default ADSL2+ line profile: 1 ● Default ADSL2+ alarm profile: 1	-
Service virtual port	● Service port ID: – Enterprise user 1: 0 – Enterprise user 2: 1 – Enterprise user 3: 2 – Enterprise user 4: 3 ● VPI: 0 ● VCI: 35 ● ID of the traffic profile in Rx direction: 10 ● ID of the traffic profile in Tx direction: 10	● The VPI/VCI is the same as the management VPI/VCI on the peer modem. ● The traffic profile that meets the service requirement is used.

Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Create VLANs.

The outer VLAN IDs are 60 and 61, and the VLANs are smart VLANs.

```
huawei(config)#vlan 60-61 smart
  It will take several minutes, and console may be timeout, please use command
idle-timeout to set time limit
  Are you sure to add VLANs? (y/n)[n]:y
```

Step 2 Set the VLAN attribute to stacking.

```
huawei(config)#vlan attrib 60-61 stacking
  It will take several minutes, and console may be timeout, please use command
idle-timeout to set time limit
  Are you sure to continue? (y/n)[n]:y
```

Step 3 Add an upstream port to the VLANs.

Add upstream port 0/19/0 to VLANs 60 and 61.

```
huawei(config)#port vlan 60-61 0/19 0
  It will take several minutes, and console may be timeout, please use command
idle-timeout to set time limit
  Are you sure to add standard port(s)? (y/n)[n]:y
  The total of the VLANs having been processed is 2
  The total of the port VLAN(s) having been added is 2
```

Step 4 Add a traffic profile.

The profile ID is 10, the CIR is 2 Mbit/s, and packets are scheduled according to the priority specified in the traffic profile.

huawei(config)#**traffic table ip index 10 cir 2048 priority user-cos 4 priority-policy local-Setting**

Step 5 Activate the ADSL2+ port and bind a profile to it.

Use the default ADSL2+ line profile 1. Activate the ADSL2+ port and bind alarm profile 1 to the port. The following uses port 0/2/0 as an example. The configuration of the other three ADSL2+ ports are similar to that of port 0/2/0.

NOTE

- By default, the port is in the activated state. Before binding a profile to the port, you must deactivate the port.

```
huawei(config)#interface adsl 0/2
huawei(config-if-adsl-0/2)#deactivate 0
huawei(config-if-adsl-0/2)#activate 0 template-index 1
huawei(config-if-adsl-0/2)#alarm-config 0 1
huawei(config-if-adsl-0/2)#quit
```

Step 6 Add service ports to the VLANs.

Add service ports to the VLANs, and use traffic profile 10 that meets the service requirements. The VPI and the VCI are 0 and 35 respectively, the same as those on the peer modem.

```
huawei(config)#service-port 0 vlan 60 adsl 0/2/0 vpi 0 vci 35 rx-cttr 10 tx-cttr
10
huawei(config)#service-port 1 vlan 60 adsl 0/2/1 vpi 0 vci 35 rx-cttr 10 tx-cttr
10
huawei(config)#service-port 2 vlan 61 adsl 0/3/0 vpi 0 vci 35 rx-cttr 10 tx-cttr
10
huawei(config)#service-port 3 vlan 61 adsl 0/3/1 vpi 0 vci 35 rx-cttr 10 tx-cttr 10
```

Step 7 Set the inner VLAN tags.

Copyright © Huawei Technologies Co., Ltd.

The inner VLAN tag identifies the user. Note that the inner VLAN tag must be unique in one ISP domain, and the inner VLAN tags can be the same in different ISP domains.

```
huawei(config)#stacking label service-port 0 11
huawei(config)#stacking label service-port 1 12
huawei(config)#stacking label service-port 2 11
huawei(config)#stacking label service-port 3 12
```

Step 8 Save the data.

```
huawei(config)#save
```

----End

Result

- After passing the authentication by the ISP1 BRAS, enterprise 1 and enterprise 2 can obtain the service provided by ISP1.
- After passing the authentication by the ISP2 BRAS, enterprise 3 and enterprise 4 can obtain the service provided by ISP2.

Configuration File

```
vlan 60-61 smart
  It will take several minutes, and console may be timeout, please use command
idle-timeout to set time limit
  Are you sure to add VLANs? (y/n)[n]:y
  The total of the VLANs having been processed is 2
  The total of the added VLANs is 2

vlan attrib 60-61 stacking
  It will take several minutes, and console may be timeout, please use command
idle-timeout to set time limit
  Are you sure to continue? (y/n)[n]:y
  The total of the VLANs having been processed is 2
  The total of the VLAN(s) which have been operated successfully is 2
port vlan 60-61 0/19 0
    It will take several minutes, and console may be timeout, please use command
idle-timeout to set time limit
  Are you sure to add standard port(s)? (y/n)[n]:y
  The total of the VLANs having been processed is 2
  The total of the port VLAN(s) having been added is 2
traffic table ip index 100 cir 2048 priority user-cos 4 priority-policy local-
Setting
 service-port 0 vlan 60 adsl 0/2/0 vpi 0 vci 35 rx-cttr 10 tx-cttr 10
service-port 1 vlan 60 adsl 0/2/1 vpi 0 vci 35 rx-cttr 10 tx-cttr 10
service-port 2 vlan 61 adsl 0/3/0 vpi 0 vci 35 rx-cttr 10 tx-cttr 10
service-port 3 vlan 61 adsl 0/3/0 vpi 0 vci 35 rx-cttr 10 tx-cttr 10
stacking label service-port 0 11
stacking label service-port 1 12
stacking label service-port 2 11
stacking label service-port 3 12
save
```

4.3 Configuration Example of the PWE3 Private Line Service

This topic describes how to configure the MPLS PWE3 private line service using examples.

Copyright © Huawei Technologies Co., Ltd.

Context

For the PWE3 service model and network application, see Configuring the PWE3 Private Line Service.

PWE3 encapsulation may be performed in the following typical scenarios based on user-side service types and upstream network types.

User-Side Service	Upstream Network	Application
ATM	IP	Mainly used for the ATM network reconstruction. When the IP protocol is deployed for the transmission network and the ATM network evolves to the IP network, PWE3 encapsulation is recommended.
ATM	MPLS	Mainly used for the ATM network reconstruction. When the MPLS protocol is deployed for the transmission network and the ATM network evolves to the IP network, PWE3 encapsulation is recommended.
ETH	MPLS	Mainly used for private network data interaction between different enterprise branches.
TDM	IP	Mainly used to integrate the TDM circuit into the packet switched network (PSN) to provide more value-added services. When the IP protocol is deployed for the transmission network and the IP network provides simulated TDM services, PWE3 encapsulation is recommended.
TDM	MPLS	Mainly used to integrate the TDM circuit into the PSN to provide more value-added services. When the MPLS protocol is deployed for the transmission network and the IP network provides simulated TDM services, PWE3 encapsulation is recommended.

4.3.1 Example: Configuring ATM PWE3 to Implement Migration from ATM Network to IP Network

ATM PWE3 applies to ATM network reconstruction. If the IP protocol is used in the transport network, ATM PWE3 is recommended to migrate the ATM network to an IP network.

Service Requirements

- The original ATM DSLAM is replaced by the MA5600T/MA5603T/MA5608T and the upper-layer ATM BRAS remains.
- ATM service data is transparently transmitted across the network.
- The quality of service (QoS) such as traffic and priority, can be guaranteed for real-time ATM services.

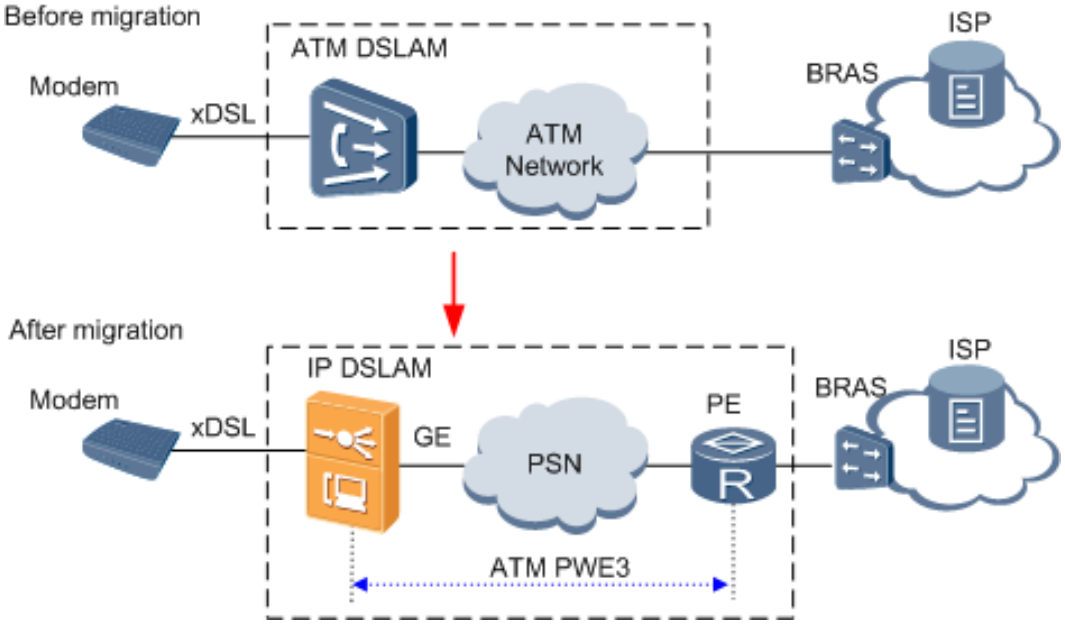
Copyright © Huawei Technologies Co., Ltd.

Networking

Figure 4-3 shows an example network of the ATM PWE3.

- Users access to MA5600T/MA5603T/MA5608T using xDSL service boards.
- The PW encapsulation mode is used to enable the transparent transmission of data over the IP network.
- PWs in the Ntol mode are used. Specifically, one PW is bound to multiple PVCs so that the same service from multiple users is carried by the same PW.
- In the upstream direction, the trTCM by CoS remarking based on PWs is used; in the downstream direction, the early drop based on CoS threshold is used. In this way, QoS can be guaranteed for various services.

Figure 4-3 Example network of the ATM PWE3



Prerequisite

- The xDSL board and the SPUB board must be in position and must work in the normal state.
- The static routing protocol or the OSPF protocol must be successfully configured on each device in the network (the host route of each port must be successfully advertised).

Context

For the principle and configuration of trTCM by CoS remarking, see Configuring PW-based trTCM by CoS Remarking.

The following ATM service types are available:

Copyright © Huawei Technologies Co., Ltd.

- Unspecified bit rate (UBR): UBR services support non-real-time applications, such as file transferring and Email. These applications have low requirements on delay or delay changes.
- Variable bit rate (VBR): VBR services can be further classified into real-time variable bit rate (rt-VBR) services and non-real-time variable bit rate (nrt-VBR) services. Both rt-VBR and nrt-VBR services support changeable (burst) cell transmitting rate at the source end. The rt-VBR service type mainly applies to voice and video services.
- Constant bit rate (CBR): The CBR service type usually applies to real-time services that have high requirements on delay changes. Such services include voice, video, and circuit emulation services.

Data Plan

Table 4-3 lists the data plan for configuring the ATM PWE3.

Table 4-3 Key data plan for configuring the ATM PWE3

Item	Data	Remarks
MPLS	LSR ID: 5.5.5.5	The LSR ID must be the same as the IP address of the loopback interface on the device. To differentiate between the LSR ID and other IP addresses, set the LSR ID to a special unique value so that it identifies the device intuitively. The MPLS feature must be enabled for: 1. Global 2. L2VPN 3. VLAN and VLAN interfaces
VLAN	Smart VLAN: 300 IP address of the VLAN interface: 192.168.1.20 Upstream port: 0/19/1	VLAN and VLAN interfaces must be configured to enable MPLS forwarding.
PW parameters	Peer IP address: 7.7.7.7 PW type: ATM Nto1 VCC Control word: enabled (Optional) Maximum number of concatenated ATM cells: 4 (Optional) Maximum encapsulation delay of ATM cells: 10 ms PW type: static	The control word adds control information into service packets to rearrange the packets and to prevent packet disorder. ATM services must use the control word since they have high requirements on time sequence. Cell concatenation enables a PW packet to carry multiple ATM cells. In this way, the transmission efficiency of ATM cells over a PSN network and bandwidth utilization are improved.

Copyright © Huawei Technologies Co., Ltd.

Item	Data	Remarks
Tunnel	Tunnel ID: 20; tunnel interface ID: 20 Encapsulation protocol of the tunnel interface at the data link layer: MPLS IP Source IP address of the tunnel: 5.5.5.5 Destination IP address of the tunnel: 7.7.7.7	IP tunnels are used. Ingress and egress addresses of a tunnel are the LSR IDs of the local device and the peer PE device, respectively.
OSPF	OSPF process ID: 200; OSPF area ID: 1	Routes use the OSPF protocol.
PWE3 gateway	LSR ID: 7.7.7.7	It is the LSR ID of the peer PE device.

Table 4-4 Plan for configuring attributes of each type of service

Item	service Type			Remarks
	UBR	VBR	CBR	
Board Slot	0/2	0/3	0/4	Multiple services of the same type but from different users are deployed at different ports on the same board (in the same slot). By doing so, the same PW is used to carry multiple PVCs. This improves the transmission efficiency, reduces the number of PWs required, and facilitates the application of QoS policies. Services of different types are deployed on boards in different slots, isolating the services physically.
VPI/ VCI of Cells	0/35	0/35	0/35	Since the services belong to the same ISP, the VPI/VCI parameters of cells on PVCs at different ports are the same.
Binding PW ID	20	21	22	Services of different types are carried over different PWs, eliminating service interaction.

Copyright © Huawei Technologies Co., Ltd.

Item	service Type			Remarks
	UBR	VBR	CBR	
Initial Value for Ingress PVC in the PW	0/32	0/33	0/34	Since the VPI/VCI parameters of cells on PVCs at different ports are the same, the VPI/VCI parameters must be changed once before the cells on client-side PVCs are encapsulated into PWs. This ensures that the VPI/VCI parameters are unique for cells on each PVC in the PW.
Initial Value for Egress PVC in the PW	1/32	1/33	1/34	
Egress Label of the PW	8450	8451	8452	
Ingress Label of the PW	8460	8461	8462	
PW CAR	12288 Kbit/s	30720 Kbit/s	6144 Kbit/s	QoS policies: In the upstream direction, priorities of service packets are remarked by setting CAR and PIR for the PW and only yellow packets are identified (CAR < Rate < PIR).
User-CoS Priority	1	4	5	
CoS Priority After Remarking	0	2	5	
WRED Profile	ID: 5	ID: 5	ID: 5	QoS policies: In the downstream direction, the xDSL board sets CoS drop threshold globally to early drop yellow packets.

Copyright © Huawei Technologies Co., Ltd.

Item	service Type			Remarks
	UBR	VBR	CBR	
Traffic Profile	● CAR: OFF ● Color policy: cos-remark ● Downstream priority policy: tag-in-package	● CAR: OFF ● Color policy: cos-remark ● Downstream priority policy: tag-in-package	● CAR: OFF ● Color policy: cos-remark ● Downstream priority policy: tag-in-package	The traffic profile does no limit the rate. Instead the rate is limited using PWs.

Procedure

Step 1 Configure a VLAN and add an upstream port to the VLAN.

Create upstream VLAN 300 and add upstream port 0/19/1 to VLAN 300.

```
huawei(config)#vlan 300 standard
 huawei(config)#port vlan 300 0/19 1
```

Step 2 Enable MPLS.

1. Configure the IP address of the loopback interface.

   Configure the IP address of loopback interface 0 to 5.5.5.5/32.

   ```
   huawei(config)#interface loopback 0
   huawei(config-if-loopback0)#ip address 5.5.5.5 32
   huawei(config-if-loopback0)#quit
   ```

2. Configure the LSR ID of the MPLS and enable global MPLS function and Layer 2 VPN.

   ```
   huawei(config)#mpls lsr-id 5.5.5.5
   huawei(config)#mpls
   huawei(config-mpls)#quit
   huawei(config)#mpls l2vpn
   ```

3. Enable the MPLS function for VLAN 300, configure the IP address of the VLAN interface 300, and enable the MPLS function for it.

   ```
   huawei(config)#mpls vlan 300
   huawei(config)#interface vlanif 300
   huawei(config-if-vlanif300)#ip address 192.168.1.20 24
   huawei(config-if-vlanif300)#mpls
   huawei(config-if-vlanif300)#quit
   ```

Step 3 Configure a route.

PWE3 has no special requirement for the routing policy. Either a static route or an OSPF dynamic route can be configured. Because OSPF supports MPLS RSVP-TE extension, an OSPF dynamic route is recommended.

```
huawei(config)#ospf 1
huawei(config-ospf-1)#area 200
```


Copyright © Huawei Technologies Co., Ltd.

```
huawei(config-ospf-1-area-0.0.0.200)#network 192.168.1.0 0.0.0.255
huawei(config-ospf-1-area-0.0.0.200)#network 5.5.5.5 0.0.0.0
huawei(config-ospf-1-area-0.0.0.200)#return
```

Step 4 Configure a PWE3 outer tunnel.

Configure the tunnel ID to 20 and the encapsulation protocol of the tunnel interface at the data link layer to MPLS IP.

```
huawei#config
huawei(config)#interface tunnel 20
huawei(config-if-tunnel20)#tunnel-protocol mpls ip
```

Configure the source IP address of the tunnel to 5.5.5.5.

```
huawei(config-if-tunnel20)#source 5.5.5.5
```

Configure the destination IP address of the tunnel to 7.7.7.7.

```
huawei(config-if-tunnel20)#destination 7.7.7.7
huawei(config-if-tunnel20)#quit
```

Step 5 Configure the tunnel policy.

Configure the policy name to atmpw-plcy.

```
huawei(config)#tunnel-policy atmpw-plcy
Info: New tunnel-policy is configured.
huawei(config-tunnel-policy-atmpw-plcy)#tunnel select-seq ip load-balance-number
1
huawei(config-tunnel-policy-atmpw-plcy)#quit
```

Step 6 Configure the PW parameters.

NOTE

Take the configuration of PW 20 for example. To configure the PW 21 and PW 22 based on the data plan using the same steps.

1. Configure the PW ID to 20.
   ```
   huawei(config)#pw-para 20
   ```
2. Configure the LSR ID of the peer PWE3 gateway in the PW. Configure the LSR ID of the PWE3 gateway to 7.7.7.7.
   ```
   huawei(config-pw-para-20)#peer-address 7.7.7.7
   ```
3. Configure the PW type to ATM NTo1 VCC.
   ```
   huawei(config-pw-para-20)#pw-type atm nto1 vcc
   ```
4. Configure the PW to support the control word.
   ```
   huawei(config-pw-para-20)#control-word
   ```
5. (Optional) Set the maximum number of concatenated ATM cells to 4.
   ```
   huawei(config-pw-para-1)#max-atm-cells 4
   ```
6. (Optional) Set the maximum encapsulation delay of ATM cells to 10 ms.
   ```
   huawei(config-pw-para-1)#max-encapcell-delay 10
   ```
7. Configure the tunnel policy used by the PW.

   Configure the tunnel policy name to atmpw-plcy.
   ```
   huawei(config-pw-para-20)#tnl-policy atmpw-plcy huawei(config-pw-para-20)#quit
   ```

Step 7 Configure a traffic profile.

1. For UBR services, set the upstream/downstream traffic profile to 20, CIR to off (limiting rate only on BRAS), color policy to CoS, user-side packet mapping mode to outer-layer 802.1p, default 802.1p to 1, and priority policy to **tag-in-package**.

Copyright © Huawei Technologies Co., Ltd.

```
huawei(config)#traffic table ip index 20 cir off color-policy cos priority
user-cos 1 priority-policy tag-in-package
```

NOTE

- The color policy in the upstream and downstream traffic profiles must be the same.
- If the color policy is cos-remark, the priority policy must be tag-in-package for the downstream direction.

2. For VBR services, set the upstream traffic profile to 21, CIR to off, color policy to CoS, user-side packet mapping mode to outer-layer 802.1p, default 802.1p to 4, and priority policy to **tag-in-package**.

```
huawei(config)#traffic table ip index 21 cir off color-policy cos priority
user-cos 4 priority-policy tag-in-package
```

3. For CBR services, set the upstream traffic profile to 22, CIR to off, color policy to CoS, user-side packet mapping mode to outer-layer 802.1p, default 802.1p to 5, and priority policy to **tag-in-package**.

```
huawei(config)#traffic table ip index 22 cir off color-policy cos priority
user-cos 5 priority-policy tag-in-package
```

Step 8 Create an ATM access service stream.

ATM cells must be encapsulated into ATM over Ethernet (AOE) packets before being carried by PWs. That is, create an ATM service stream.

- Create AOE service streams in batches for UBR services.

  The service board is in slot 0/2, VPI/VCI is 0/35, and the traffic profile for the upstream and downstream directions is 20.

```
huawei(config)#multi-service-port vlan aoe board 2 vpi 0 vci 35 inbound
traffic-table index 20 outbound traffic-table index 20
```

- Create AOE service streams in batches for VBR services.

  The service board is in slot 0/3, VPI/VCI is 0/35, and the traffic profile for the upstream and downstream directions is 21.

```
huawei(config)#multi-service-port vlan aoe board 3 vpi 0 vci 35 inbound
traffic-table index 21 outbound traffic-table index 21
```

- Create AOE service streams in batches for CBR services.

  The service board is in slot 0/4, VPI/VCI is 0/35, and the traffic profile for the upstream and downstream directions is 22.

```
huawei(config)#multi-service-port vlan aoe board 4 vpi 0 vci 35 inbound
traffic-table index 22 outbound traffic-table index 22
```

Step 9 Bind the PVCs to PW 20 in batches to create an ATM PWE3 service.

Since the VPI/VCI parameters of cells on PVCs at different ports are the same, the VPI/VCI parameters must be changed once before the cells on client-side PVCs are encapsulated into PWs. This ensures that the VPI/VCI parameters are unique for cells on each PVC in the PW.

- Bind PVCs and PWs in batches for UBR services.

```
huawei(config)#multi-pw-ac-binding pvc board 2 vpi 0 vci 35 from-outvpi 0 outvci
32
from-invpi 1 invci 32 pw 20 static transmit-label 8450 receive-label 8460
```

- Bind PVCs and PWs in batches for VBR services.

```
huawei(config)#multi-pw-ac-binding pvc board 3 vpi 0 vci 35 from-outvpi 0 outvci
33
from-invpi 1 invci 33 pw 21 static transmit-label 8451 receive-label 8461
```

- Bind PVCs and PWs in batches for CBR services.

```
huawei(config)#multi-pw-ac-binding pvc board 4 vpi 0 vci 35 from-outvpi 0 outvci
34
from-invpi 1 invci 34 pw 22 static transmit-label 8452 receive-label 8462
```


Copyright © Huawei Technologies Co., Ltd.

Step 10 Configure the WRED profile.

The index is 5. Configure the WRED profile so that green packets are not dropped, lower threshold for dropping yellow packets is 50, upper threshold for dropping yellow packets is 80, and the packet dropping percentage is 100.

```
huawei(config)#wred-profile index 5 green low-limit 100 high-limit 100
discard-probability 0 yellow low-limit 50 high-limit 80 discard-probability 100
```

Step 11 Configure queues and bind the WRED profile.

```
huawei(config)#queue-wred queue0 5 queue1 5 queue2 5 queue3 5 queue4 5 queue5 5
queue6 5 queue7 5
```

Step 12 Configure the priority remarking policy.

Remark the priority of yellow packets. Specifically, remark priority 1 (UBR service packets) to 0; priority 4 (VBR service packets) to 2, and priority 5 (CBR service packets) to 5.

```
huawei(config)#cos-remark cos1 0 cos4 2 cos5 5
```

Step 13 Configure the mapping between queues and 802.1p priorities.

Packets with 802.1p priorities 0 and 1 join queue 1; packets with 802.1p priorities 2 and 4 join queue 4; packets with 802.1p priority 5 join queue 5.

NOTE

Ensure that the packets with the CoS values before and after remarking join the same queue.

```
huawei(config)#cos-queue-map cos0 1 cos1 1 cos2 4 cos4 4 cos5 5
```

Step 14 Set committed rate in the PW upstream direction.

- Set CAR in the upstream direction of PW 20 to 12288 kbit/s.
  ```
  huawei(config)#mpls car-pw 20 cir 12288
  ```
- Set CAR in the upstream direction of PW 21 to 30720 kbit/s.
  ```
  huawei(config)#mpls car-pw 21 cir 30720
  ```
- Set CAR in the upstream direction of PW 22 to 6144 kbit/s.
  ```
  huawei(config)#mpls car-pw 22 cir 6144
  ```

----End

Result

- UBR, VBR, and CBR services can be migrated to an IP network smoothly. No change is required on the user side and users will not feel any change.
- Various services are scheduled based on their priorities. When a congestion occurs on the network, the quality of CBR services is guaranteed with precedence.
- When a congestion occurs at a port, the system first drops traffic of the burst bandwidth (bandwidth > peak value), ensuring the guaranteed bandwidth for each type of service.

Configuration File

```
vlan 300 smart
port vlan 300 0/19 1
interface loopback 0
ip address 5.5.5.5 32
quit
mpls lsr-id 5.5.5.5
mpls
quit
mpls l2vpn
mpls vlan 300
interface vlanif 300
```


Copyright © Huawei Technologies Co., Ltd.

```
ip address 192.168.1.20 24
mpls
quit
ospf 1
area 200
network 192.168.1.0 0.0.0.255
network 5.5.5.5 0.0.0.0
return
config
interface tunnel 20
tunnel-protocol mpls ip
destination 7.7.7.7
quit
tunnel-policy atmpw-plcy
tunnel select-seq ip load-balance-number 1
quit
pw-para 20
peer-address 7.7.7.7
pw-type atm nto1 vcc
control-word
max-atm-cells 4
max-encapcell-delay 10
tnl-policy atmpw-plcy
quit
traffic table ip index 20 cir off color-policy cos priority user
-cos 1 priority-policy tag-in-package
traffic table ip index 21 cir off color-policy cos priority user
-cos 4 priority-policy tag-in-package
traffic table ip index 22 cir off color-policy cos priority user
-cos 5 priority-policy tag-in-package
multi-service-port vlan aoe board 2 vpi 0 vci 35 inbound traffi
c-table index 20 outbound traffic-table index 20
multi-service-port vlan aoe board 3 vpi 0 vci 35 inbound traffi
c-table index 21 outbound traffic-table index 21
multi-service-port vlan aoe board 4 vpi 0 vci 35 inbound traffi
c-table index 22 outbound traffic-table index 22
multi-pw-ac-binding pvc board 2 vpi 0 vci 35 from-outvpi 0 outvci 32
from-invpi 1 invci 32 pw 20 static transmit-label 8450 receive-label 8460
multi-pw-ac-binding pvc board 3 vpi 0 vci 35 from-outvpi 0 outvci 33
from-invpi 1 invci 33 pw 21 static transmit-label 8451 receive-label 8461
multi-pw-ac-binding pvc board 4 vpi 0 vci 35 from-outvpi 0 outvci 34
from-invpi 1 invci 34 pw 22 static transmit-label 8452 receive-label 8462
wred-profile index 5 green low-limit 100 high-limit 100 discard-probability
 0 yellow low-limit 50 high-limit 80 discard-probability 100
queue-wred queue0 5 queue1 5 queue2 5 queue3 5 queue4 5 queue5 5
queue6 5 queue7 5
cos-remark cos1 0 cos4 2 cos5 5
cos-queue-map cos0 1 cos1 1 cos2 4 cos4 4 cos5 5
mpls car-pw 20 cir 12288
mpls car-pw 20 cir 30720
mpls car-pw 20 cir 6144
```

4.3.2 Example: Configuring the ATM PWE3 to Achieve emulated ATM Services on the MPLS Network

ATM PWE3 is mainly used in ATM network reconstruction. When the MPLS protocol is deployed for the transmission network and the ATM network evolves to the MPLS network, PWE3 encapsulation is recommended.

Service Requirements

- The xDSL service board (or AIUG board) of the MA5600T/MA5603T/MA5608T is used to provide the ATM service.

Copyright © Huawei Technologies Co., Ltd.

- The PW encapsulation mode is adopted so that data can be transparently transmitted in the MPLS network.

Prerequisite

- The xDSL board (or AIUG board) and the SPUB board must be in position and must work in the normal state.
- The static routing protocol or the OSPF protocol must be successfully configured on each device in the network (the host route of each port must be successfully advertised).

Context

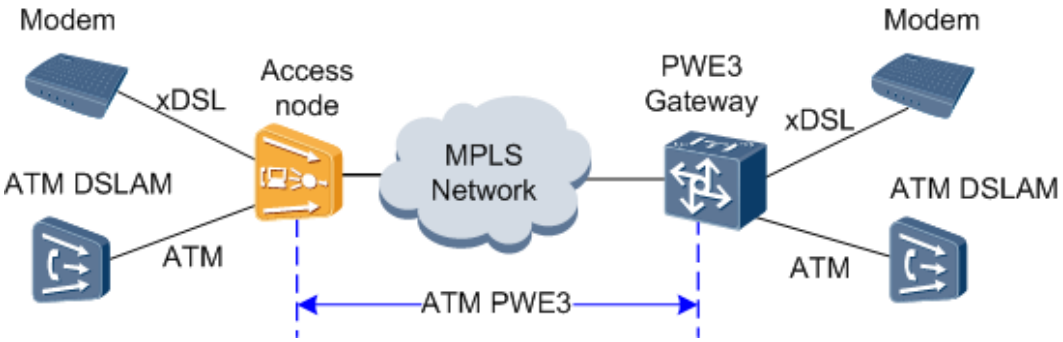
The implementation process of the ATM PWE3 (MPLS-based) is as follows:

1. The xDSL modem or ATM DSLAM transmits the ATM service to the xDSL or AIUG board of the MA5600T/MA5603T/MA5608T.
2. The control board sends ATM packets to the SPUB board.
3. After performing the PW and MPLS encapsulation for the packets, the SPUB board performs the MPLS packet header encapsulation and then sends them to the control board.
4. The control board performs the Layer 2 forwarding and sends the packets to the upstream port.
5. The packets are sent over the MPLS network to the peer PWE3 gateway (such as the PTN).
6. The PWE3 gateway restores the ATM cells and sends them to the peer ATM device.

Networking

Figure 4-4 shows an example network of the ATM PWE3 (MPLS-based).

Figure 4-4 Example network of the ATM PWE3 (MPLS-based)



Data Plan

Table 4-5 lists the data plan for configuring the ATM PWE3 (MPLS-based).

Copyright © Huawei Technologies Co., Ltd.

Table 4-5 Data plan for configuring the ATM PWE3 (MPLS-based)

Item	Data
MPLS	LSR ID: 5.5.5.5 Global MPLS TE: enabled MPLS Layer 2 VPN: enabled VLAN MPLS RSVP-TE: enabled
VLAN	Standard VLAN for MPLS forwarding: 300 MPLS address of the VLAN interface: 192.168.2.20 Upstream port: 0/19/1
PW parameters	PW ID: 20 Peer IP address: 7.7.7.7 PW type: ATM Nto1 VCC PW in VPI/VCI: 0/35 PW out VPI/VCI: 8/35 PW type: static Control word: enabled PW out port: 8450 PW in port: 8460
Tunnel	Tunnel ID: 20; tunnel interface ID: 20 Encapsulation protocol of the tunnel interface at the data link layer: MPLS TE Tunnel signaling protocol: RSVP-TE
ATM service port	Port: 0/2/0 Emulation SVLAN: 3001 VPI/VCI: 0/35
OSPF	OSPF process ID: 200; OSPF area ID: 1 Enable MPLS TE for the OSPF area
PWE3 gateway	LSR ID: 7.7.7.7

Procedure

Step 1 Configure a VLAN and add an upstream port to the VLAN.

Create upstream VLAN 300 and add upstream port 0/19/1 to VLAN 300.

```
huawei(config)#vlan 300 standard
 huawei(config)#port vlan 300 0/19 1
```

Step 2 Enable MPLS.

Copyright © Huawei Technologies Co., Ltd.

1. Configure the IP address of the loopback interface.

   Configure the IP address of loopback interface 0 to 5.5.5.5/32.

   ```
   huawei(config)#interface loopback 0
   huawei(config-if-loopback0)#ip address 5.5.5.5 32
   huawei(config-if-loopback0)#quit
   ```

2. Configure the LSR ID of the MPLS and enable global MPLS TE and Layer 2 VPN.

   ```
   huawei(config)#mpls lsr-id 5.5.5.5
   huawei(config)#mpls
   huawei(config-mpls)#mpls te
   huawei(config-mpls)#mpls rsvp-te
   huawei(config-mpls)#quit
   huawei(config)#mpls l2vpn
   ```

3. Enable the VLAN interface MPLS TE function and configure the IP address of the VLAN interface.

   ```
   huawei(config)#mpls vlan 300
   huawei(config)#interface vlanif 300
   huawei(config-if-vlanif300)#ip address 192.168.2.20 24
   huawei(config-if-vlanif300)#mpls
   huawei(config-if-vlanif300)#mpls te
   huawei(config-if-vlanif300)#mpls rsvp-te
   huawei(config-if-vlanif300)#quit
   ```

Step 3 Configure a route.

PWE3 has no special requirement for the routing policy. Either a static route or an OSPF dynamic route can be configured. Because OSPF supports MPLS RSVP-TE extension, an OSPF dynamic route is recommended.

```
huawei(config)#ospf 1
huawei(config-ospf-1)#opaque-capability enable..//Enable the opaque capability
huawei(config-ospf-1)#area 200
huawei(config-ospf-1-area-0.0.0.200)#mpls-te enable standard-complying //Enable
MPLS TE for the OSPF area
huawei(config-ospf-1-area-0.0.0.200)#network 192.168.2.0 0.0.0.255
huawei(config-ospf-1-area-0.0.0.200)#network 5.5.5.5 0.0.0.0
huawei(config-ospf-1-area-0.0.0.200)#return
```

Step 4 Configure a PWE3 outer tunnel.

Configure the tunnel ID to 20 and the encapsulation protocol of the tunnel interface at the data link layer to MPLS TE.

```
huawei#config
huawei(config)#interface tunnel 20
huawei(config-if-tunnel20)#tunnel-protocol mpls te
```

Configure the destination IP address of the tunnel to 7.7.7.7.

```
huawei(config-if-tunnel10)#destination 7.7.7.7
```

Configure the ID of the MPLS TE tunnel interface to 20. The tunnel ID and LSR ID uniquely identify an MPLS TE tunnel.

```
huawei(config-if-tunnel20)#mpls te tunnel-id 20
```

Configure the signaling protocol of the MPLS TE tunnel to RSVP-TE.

```
huawei(config-if-tunnel20)#mpls te signal-protocol rsvp-te
```

Configure the MPLS TE tunnel for being bound by a VPN instance.

```
huawei(config-if-tunnel20)#mpls te reserved-for-binding
```


Copyright © Huawei Technologies Co., Ltd.

Commit the configuration and quit the tunnel configuration.

```
huawei(config-if-tunnel20)#mpls te commit
huawei(config-if-tunnel20)#quit
```

Step 5 Configure the tunnel policy.

Configure the policy name to atmpw-plcy.

```
huawei(config)#tunnel-policy atmpw-plcy
Info: New tunnel-policy is configured.
huawei(config-tunnel-policy-atmpw-plcy)#tunnel binding destination 7.7.7.7 te
tunnel 20
huawei(config-tunnel-policy-atmpw-plcy)#quit
```

Step 6 Configure the PW parameters.

NOTE

Take the configuration of PW 20 for example. To configure the PW 21 and PW 22 based on the data plan using the same steps.

1. Configure the PW ID to 20.
   ```
   huawei(config)#pw-para 20
   ```
2. Configure the LSR ID of the peer PWE3 gateway in the PW. Configure the LSR ID of the PWE3 gateway to 7.7.7.7.
   ```
   huawei(config-pw-para-20)#peer-address 7.7.7.7
   ```
3. Configure the PW type to ATM NTo1 VCC.
   ```
   huawei(config-pw-para-20)#pw-type atm nto1 vcc
   ```
4. Configure the PW to support the control word.
   ```
   huawei(config-pw-para-20)#control-word
   ```
5. (Optional) Set the maximum number of concatenated ATM cells to 4.
   ```
   huawei(config-pw-para-1)#max-atm-cells 4
   ```
6. (Optional) Set the maximum encapsulation delay of ATM cells to 10 ms.
   ```
   huawei(config-pw-para-1)#max-encapcell-delay 10
   ```
7. Configure the tunnel policy used by the PW.

   Configure the tunnel policy name to atmpw-plcy.
   ```
   huawei(config-pw-para-20)#tnl-policy atmpw-plcy huawei(config-pw-para-20)#quit
   ```

Step 7 Create an ATM access service stream.

ATM cells must be encapsulated into ATM over Ethernet (AOE) packets before being carried by PWs. That is, create an ATM service stream.

- Create AOE service streams in batches for UBR services.

  The service board is in slot 0/2, VPI/VCI is 0/35, and the traffic profile for the upstream and downstream directions is 20.
  ```
  huawei(config)#multi-service-port vlan aoe board 2 vpi 0 vci 35 inbound
  traffic-table index 20 outbound traffic-table index 20
  ```
- Create AOE service streams in batches for VBR services.

  The service board is in slot 0/3, VPI/VCI is 0/35, and the traffic profile for the upstream and downstream directions is 21.
  ```
  huawei(config)#multi-service-port vlan aoe board 3 vpi 0 vci 35 inbound
  traffic-table index 21 outbound traffic-table index 21
  ```
- Create AOE service streams in batches for CBR services.

  The service board is in slot 0/4, VPI/VCI is 0/35, and the traffic profile for the upstream and downstream directions is 22.

Copyright © Huawei Technologies Co., Ltd.

```
huawei(config)#multi-service-port vlan aoe board 4 vpi 0 vci 35 inbound
traffic-table index 22 outbound traffic-table index 22
```

Step 8 Bind the PVCs to PW 20 in batches to create an ATM PWE3 service.

Since the VPI/VCI parameters of cells on PVCs at different ports are the same, the VPI/VCI parameters must be changed once before the cells on client-side PVCs are encapsulated into PWs. This ensures that the VPI/VCI parameters are unique for cells on each PVC in the PW.

- Bind PVCs and PWs in batches for UBR services.

```
huawei(config)#multi-pw-ac-binding pvc board 2 vpi 0 vci 35 from-outvpi 0 outvci
32
from-invpi 1 invci 32 pw 20 static transmit-label 8450 receive-label 8460
```

- Bind PVCs and PWs in batches for VBR services.

```
huawei(config)#multi-pw-ac-binding pvc board 3 vpi 0 vci 35 from-outvpi 0 outvci
33
from-invpi 1 invci 33 pw 21 static transmit-label 8451 receive-label 8461
```

- Bind PVCs and PWs in batches for CBR services.

```
huawei(config)#multi-pw-ac-binding pvc board 4 vpi 0 vci 35 from-outvpi 0 outvci
34
from-invpi 1 invci 34 pw 22 static transmit-label 8452 receive-label 8462
```

Step 9 Query the PW status.

```
huawei(config)#display pw-ac-binding pvc 0/2/0 vpi 0 vci 35
  Total : 1  (Up/Down :    1/0           Static/LDP :    1/0)
  ------------------------------------------------------------------------------
  F/S/P            PW         PW    PROTO  RECEIVE TRNS    PW
  VPIVCI           ID         STATE TYPE   LABEL   LABEL   INDEX
  ------------------------------------------------------------------------------
   0/2/0 0 35      20         up    static 8460    8450    20
  ------------------------------------------------------------------------------
  Note  : F--Frame, S--Slot, P--Port
          *: Secondary
```

----End

Result

The ATM packets can be transparently transmitted in the MPLS network and the ATM-based services can be provided normally.

Configuration File

```
vlan 300 standard
port vlan 300 0/19 1
interface loopback 0
ip address 5.5.5.5 32
quit
mpls lsr-id 5.5.5.5
mpls
mpls te
mpls rsvp-te
quit
mpls l2vpn
mpls vlan 300
interface vlanif 300
ip address 192.168.2.20 24
mpls
mpls te
mpls rsvp-te
quit
ospf 1
opaque-capability enable
area 200
```


Copyright © Huawei Technologies Co., Ltd.

```
mpls-te enable standard-complying
network 192.168.2.0 0.0.0.255
network 5.5.5.5 0.0.0.0
return
config
interface tunnel 20
tunnel-protocol mpls te
destination 7.7.7.7
mpls te tunnel-id 20
mpls te signal-protocol rsvp-te
mpls te reserved-for-binding
mpls te commit
quit
tunnel-policy atmpw-plcy
tunnel binding destination 7.7.7.7 te tunnel 20
quit
pw-para 20
peer-address 7.7.7.7
pw-type atm nto1 vcc
control-word
vccv cc cw alert ttl cv lsp-ping
tnl-policy atmpw-plcy
quit
service-port vlan aoe adsl 0/2/0 vpi 0 vci 35 rx-cttr 6 tx-cttr 6   //xDSL access
service-port vlan aoe atm 0/2/0 vpi 0 vci 35 rx-cttr 6 tx-cttr 6   //ATM access
pw-ac-bnding pvc 0/2/0 vpi 0 vci 35 outvpi 8 outvci 35 pw 20
static transmit-label 8450 receive-label 8460
```

4.3.3 Example: Configuring the ETH PWE3 to Emulate Ethernet Services on the MPLS Network

The MA5600T/MA5603T/MA5608T supports the PW encapsulation for ethernet packets and implements the ETH PWE3 emulation service after the MPLS encapsulation of the packets, providing the solution of emulation Ethernet private line service over the MPLS network.

Service Requirements

- The data interaction between enterprise branches in different regions is achieved through the metropolitan area network (MAN) that is running the MPLS protocol.
- The Ethernet service data of the enterprise private network is transparently transmitted so that the data security can be ensured.

Prerequisite

- The SPUB board must be in position and must work in the normal state.
- The static routing protocol or the OSPF protocol must be successfully configured on each device in the network (the host route of each port must be successfully advertised).

Context

The Ethernet packet-based data interaction between enterprise branches in different regions is achieved using the routers of the public network to forward the packets. If the public network uses the MPLS protocol, the Ethernet packets cannot be forwarded directly. In this case, the Ethernet packet forwarding can be achieved by using the ETH PWE3 technology. In addition, the ETH PWE3 technology can be deployed to achieve high security with low costs.

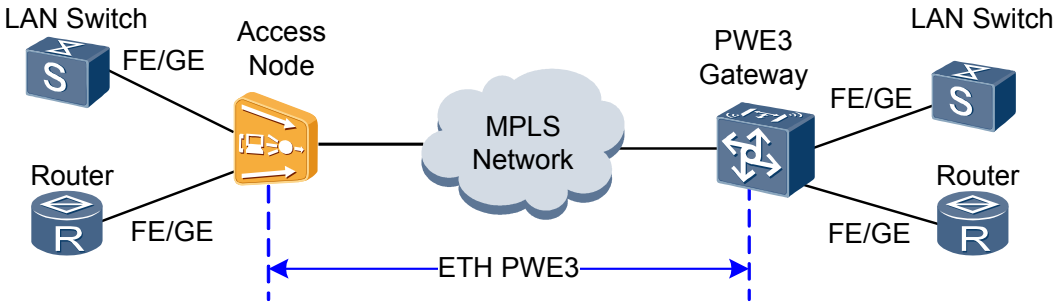
Copyright © Huawei Technologies Co., Ltd.

Networking

Figure 4-5 shows an example network of the ETH PWE3.

1. The Ethernet switch or router of the enterprise aggregates the private network data of the enterprise and sends the data to the ETH board of the MA5600T/MA5603T/MA5608T.
2. The control board sends ETH packets to the SPUB board.
3. After performing the PW and MPLS encapsulation for the packets, the SPUB board performs the ETH packet header encapsulation and then sends them to the control board.
4. The control board performs the Layer 2 forwarding and sends the packets to the upstream port.
5. The packets are sent over the MPLS network to the peer PWE3 gateway (such as the PTN).
6. The PWE3 gateway restores ETH signals and sends them to the peer Ethernet switch or router.

Figure 4-5 Example network of the ETH PWE3



Data Plan

Table 4-6 lists the data plan for configuring the ETH PWE3.

Table 4-6 Data plan for configuring the ETH PWE3

Item	Data
MPLS	LSR ID: 5.5.5.5 Global MPLS TE: enabled MPLS Layer 2 VPN: enabled VLAN MPLS RSVP-TE: enabled
VLAN	Standard VLAN for MPLS forwarding: 200 IP address of the VLAN interface: 192.168.1.10 Upstream port: 0/19/0

Copyright © Huawei Technologies Co., Ltd.

Item	Data
PW parameters	PW ID: 10 Peer IP address: 6.6.6.6 PW type: ETH tagged Control word: enabled Out label: 8500 In label: 8600
Tunnel	Tunnel ID: 10; tunnel interface ID: 10 Encapsulation protocol of the tunnel interface at the data link layer: MPLS TE Tunnel signaling protocol: RSVP-TE
ETH service port	Port: 0/4/0 Emulation SVLAN: 3001 CVLAN: 20
OSPF	OSPF process ID: 100; OSPF area ID: 1 Enable MPLS TE for the OSPF area
PWE3 gateway	LSR ID: 6.6.6.6

Procedure

Step 1 Configure a VLAN and add an upstream port to the VLAN.

Create upstream VLAN 200 and add upstream port 0/19/0 to VLAN 200.

```
huawei(config)#vlan 200 standard
huawei(config)#port vlan 200 0/19 0
```

Step 2 Enable MPLS.

1. Configure the IP address of the loopback interface.

   Configure the IP address of loopback interface 0 to 5.5.5.5/32.

   ```
   huawei(config)#interface loopback 0
   huawei(config-if-loopback0)#ip address 5.5.5.5 32
   huawei(config-if-loopback0)#quit
   ```

2. Configure the LSR ID of the MPLS and enable global MPLS TE and Layer 2 VPN.

   ```
   huawei(config)#mpls lsr-id 5.5.5.5
   huawei(config)#mpls
   huawei(config-mpls)#mpls te
   huawei(config-mpls)#mpls rsvp-te
   huawei(config-mpls)#quit
   huawei(config)#mpls l2vpn
   ```

3. Enable the VLAN interface MPLS TE function and configure the IP address of the VLAN interface.

   ```
   huawei(config)#mpls vlan 200
   huawei(config)#interface vlanif 200
   huawei(config-if-vlanif200)#ip address 192.168.1.10 24
   ```


Copyright © Huawei Technologies Co., Ltd.

```
huawei(config-if-vlanif200)#mpls
huawei(config-if-vlanif200)#mpls te
huawei(config-if-vlanif200)#mpls rsvp-te
huawei(config-if-vlanif200)#quit
```

Step 3 Configure a route.

PWE3 has no special requirement for the routing policy. Either a static route or an OSPF dynamic route can be configured. Because OSPF supports MPLS RSVP-TE extension, an OSPF dynamic route is recommended.

```
huawei(config)#ospf 1
huawei(config-ospf-1)#opaque-capability enable..//Enable the opaque capability
huawei(config-ospf-1)#area 100
huawei(config-ospf-1-area-0.0.0.100)#mpls-te enable standard-complying //Enable
MPLS TE for the OSPF area
huawei(config-ospf-1-area-0.0.0.100)#network 192.168.1.0 0.0.0.255
huawei(config-ospf-1-area-0.0.0.100)#network 5.5.5.5 0.0.0.0
huawei(config-ospf-1-area-0.0.0.100)#return
```

Step 4 Configure a PWE3 outer tunnel.

Configure the tunnel ID to 10 and the encapsulation protocol of the tunnel interface at the data link layer to MPLS TE.

```
huawei#config
huawei(config)#interface tunnel 10
huawei(config-if-tunnel10)#tunnel-protocol mpls te
```

Configure the destination IP address of the tunnel to 6.6.6.6.

```
huawei(config-if-tunnel10)#destination 6.6.6.6
```

Configure the ID of the MPLS TE tunnel interface to 10. The tunnel ID and LSR ID uniquely identify an MPLS TE tunnel.

```
huawei(config-if-tunnel10)#mpls te tunnel-id 10
```

Configure the signaling protocol of the MPLS TE tunnel to RSVP-TE.

```
huawei(config-if-tunnel10)#mpls te signal-protocol rsvp-te
```

Configure the MPLS TE tunnel for being bound by a VPN instance.

```
huawei(config-if-tunnel10)#mpls te reserved-for-binding
```

Commit the configuration and quit the tunnel configuration.

```
huawei(config-if-tunnel10)#mpls te commit
huawei(config-if-tunnel10)#quit
```

Step 5 Configure the tunnel policy.

Configure the policy name to ethpw-plcy.

```
huawei(config)#tunnel-policy ethpw-plcy
Info: New tunnel-policy is configured.
huawei(config-tunnel-policy-ethpw-plcy)#tunnel binding destination 6.6.6.6 te
tunnel 10
huawei(config-tunnel-policy-ethpw-plcy)#quit
```

Step 6 Configure the PW parameters.

1. Configure the PW ID to 10.
   ```
   huawei(config)#pw-para 10
   ```


Copyright © Huawei Technologies Co., Ltd.

2. Configure the LSR ID of the peer PWE3 gateway in the PW. Configure the LSR ID of the PWE3 gateway to 6.6.6.6.
   ```
   huawei(config-pw-para-10)#peer-address 6.6.6.6
   ```
3. Configure the PW type to ethernet tagged.
   ```
   huawei(config-pw-para-10)#pw-type ethernet tagged
   ```
4. Configure the PW to support the control word.
   ```
   huawei(config-pw-para-10)#control-word
   ```
5. Enable the virtual circuit connectivity verification (VCCV) function.
   ```
   huawei(config-pw-para-10)#vccv cc cw alert ttl cv lsp-ping
   ```
6. Configure the tunnel policy used by the PW.

   Configure the tunnel policy name to ethpw-plcy.
   ```
   huawei(config-pw-para-10)#tnl-policy etnpw-plcy
   huawei(config-pw-para-10)#quit
   ```

Step 7 Create an Ethernet access service port.

Create a VLAN for the ETH emulation service (after ETH emulation, this VLAN will be restored by the peer ETH PWE3 gateway), and then create a service port for translating the CVLAN ID into the VLAN ID of the emulation service.

```
huawei(config)#vlan 3001
huawei(config)#service-port vlan 3001 eth 0/4/0 multi-service user-vlan 20 rx-cttr
6 tx-cttr 6
```

Step 8 Bind the VLAN to the PW to create the ETH PWE3 service.

Bind emulation SVLAN 3001 to PW 10, and set PW type to static PW, out label of the PW to 8500, and in label of the PW to 8600.

```
huawei(config)#pw-ac-binding vlan 3001 pw 10 static transmit-label 8500 receive-
label 8600
```

Step 9 Query the PW status.

```
huawei(config)#display pw-ac-binding vlan 3001
  Total : 1  (Up/Down :    1/0           Static/LDP :    1/0)
  ------------------------------------------------------------------------------
  VLAN             PW         PW    PROTO  RECEIVE TRNS    PW
  ID               ID         STATE TYPE   LABEL   LABEL   INDEX
  ------------------------------------------------------------------------------
   3001            10         up    static 8600    8500    10
  ------------------------------------------------------------------------------
```

----End

Result

The private network data of the enterprise can be transparently transmitted over the MPLS network, and all services in the private network can be provided normally.

Configuration File

```
vlan 200 smart
port vlan 200 0/19 0
interface loopback 0
ip address 5.5.5.5 32
quit
mpls lsr-id 5.5.5.5
mpls
mpls te
```


Copyright © Huawei Technologies Co., Ltd.

```
mpls rsvp-te
quit
mpls l2vpn
mpls vlan 200
interface vlanif 200
ip address 192.168.1.10 24
mpls
mpls te
mpls rsvp-te
quit
ospf 1
opaque-capability enable
area 100
mpls-te enable standard-complying
network 192.168.1.0 0.0.0.255
network 5.5.5.5 0.0.0.0
return
config
interface tunnel 10
tunnel-protocol mpls te
destination 6.6.6.6
mpls te tunnel-id 10
mpls te signal-protocol rsvp-te
mpls te reserved-for-binding
mpls te commit
quit
tunnel-policy ethpw-plcy
tunnel binding destination 6.6.6.6 te tunnel 10
quit
pw-para 10
peer-address 6.6.6.6
pw-type ethernet tagged
control-word
vccv cc cw alert ttl cv lsp-ping
tnl-policy ethpw-plcy
quit
vlan 3001
service-port vlan 3001 eth 0/4/0 multi-service user-vlan 20 rx-cttr 6 tx-cttr 6
pw-ac-binding vlan 3001 pw 10 static transmit-label 8500 receive-label 8600
```

4.3.4 Example: Configuring the TDM PWE3 to Emulate TDM Services on the IP Network

The MA5600T/MA5603T/MA5608T supports SAToP encapsulation for non-frame E1 signals and implements the TDM PWE3 emulation service after IP-encapsulating the signals. In this way, the MA5600T/MA5603T/MA5608T provides emulated TDM private line service over the IP network.

Service Requirements

- To make full use of legacy TDM line and equipment, and replace legacy DDN network and ISDN PRI PBX convergence network.
- To perform MPLS over IP encapsulation on the E1 data aggregated by the Nx64k private line and ISDN PRI PBX, and transmit the data upstream as IP packets to the DDN network or SDH network.

Prerequisite

- The H802EDTB board and SPUB board are installed and work in the normal state.

Copyright © Huawei Technologies Co., Ltd.

- The working mode of the H802EDTB board is set to SAToP by running the **board workmode** command.
- A static route or dynamic route is successfully configured on each device over the network so that the IP routes between LSRs are reachable.

Context

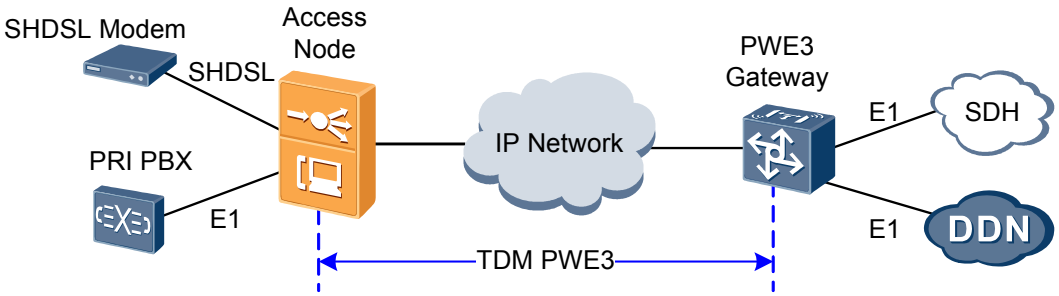
The implementation process of TDM PWE3 is as follows:

1. The data of the Nx64k private line service or ISDN PRI PBX service is converged and then transmitted to the H802EDTB board of the MA5600T/MA5603T/MA5608T.
2. After performing SAToP processing (adding CW control word and RTP header) on the E1 data, the H802EDTB board sends the data to the SPUB board through the control board.
3. After performing the PW and MPLS encapsulation on the packets, the SPUB board adds the ETH header to the packets, and then sends them to the control board.
4. The control board performs Layer 2 forwarding and sends the packets to the upstream port.
5. The packets are sent over the PSN network to the peer PWE3 gateway (such as the PTN).
6. The PWE3 gateway restores the E1 signals from the packets and then sends them to the DDN network or SDH network.

Networking

Figure 4-6 shows an example network of TDM PWE3 (IP-based).

Figure 4-6 Example network of TDM PWE3 (IP-based)



Data Plan

Table 4-7 lists the data plan for configuring TDM PWE3 (IP-based).

Table 4-7 Data plan for configuring TDM PWE3 (IP-based)

Parameter	Data
H802EDTB board	Board slot: 0/3 E1 port: 0/3/1
SPUB board	Board slot: 0/5

Copyright © Huawei Technologies Co., Ltd.

Parameter	Data
MPLS	VLAN for MPLS forwarding: VLAN 4001 IP address of VLAN interface 4001: 10.50.50.50/24 MPLS LSR ID: 3.3.3.3 Global MPLS LDP: enabled MPLS Layer 2 VPN: enabled
PW parameters	PW ID: 2 Peer IP address: 9.9.9.9 Template type: TDM SAToP E1 PW load time: 125 μs Jitter buffer size: 2500 μs Control word: enabled RTP: enabled VCCV: enabled
Tunnel	Tunnel interface ID: 10 Tunnel ID: 10 Encapsulation protocol of the tunnel interface at the data link layer: IP Policy name: **ip_policy**
Tx clock of the E1 port	Network clock, recovered from PW2

Procedure

Step 1 Configure a loopback interface.

Set the ID of the loopback interface to 0 and its IP address to 3.3.3.3/32.

```
huawei(config)#interface loopback 0
huawei(config-if-loopback0)#ip address 3.3.3.3 32
huawei(config-if-loopback0)#quit
```

Step 2 Enable basic MPLS functions.

Set the IP address of loopback interface 0 as the LSR ID.

```
huawei(config)#mpls lsr-id 3.3.3.3
```

Enable global MPLS.

```
huawei(config)#mpls
huawei(config-mpls)#lsp-trigger host  //set up an LSP by triggering the LDP through
the host address
huawei(config-mpls)#quit
```

Enable Layer 2 VPN.

```
huawei(config)#mpls l2vpn
```

Enable global LDP.

Copyright © Huawei Technologies Co., Ltd.

```
huawei(config)#mpls ldp
huawei(config-mpls-ldp)#quit
```

NOTE

- Only one session can exist between two LSRs and a local LDP session takes priority over a remote LDP session. To simplify the configuration, assume that the MA5600T/MA5603T/MA5608T is directly connected to the PTN. Hence, you need to enable only the LDP function (the local LDP session is automatically set up after the LDP function is enabled).
- If the MA5600T/MA5603T/MA5608T is not directly connected to the PTN, after the LDP function is enabled, run the **mpls ldp remote-peer** command to create an LDP remote peer and then enter the remote peer mode. Then, run the **remote-ip***ip-addr* command to specify the ID of the remote LSR.
- For detailed configurations, see Configuring the LDP LSP.

Step 3 Configure a VLAN and enable MPLS for the VLAN and the VLAN interface.

Add VLAN 4001 for forwarding MPLS packets and add an upstream port to it.

```
huawei(config)#vlan 4001 smart
huawei(config)#port vlan 4001 0/19/0
```

Enable MPLS for VLAN 4001.

```
huawei(config)#mpls vlan 4001
```

Set the IP address of VLAN interface 4001 to 10.50.50.50/24 and enable MPLS LDP for the VLAN interface.

```
huawei(config)#interface vlanif 4001
huawei(config-if-vlanif4001)#ip address 10.50.50.50 24
huawei(config-if-vlanif4001)#mpls
huawei(config-if-vlanif4001)#mpls ldp
huawei(config-if-vlanif4001)#quit
```

Step 4 Configure a route.

PWE3 has no special requirements for the routing policy. A static route, or dynamic RIP, or OSPF route can be configured. An OSPF dynamic route is recommended because OSPF supports MPLS RSVP-TE extension.

Set the OSPF process ID to 100 and OSPF area ID to 1. In addition, configure the interfaces (VLAN interface and loopback interface) that run OSPF and configure the areas of the interfaces.

```
huawei(config)#ospf 1
huawei(config-ospf-1)#area 100
huawei(config-ospf-1-area-0.0.0.100)#network 10.50.50.0 0.0.0.255
huawei(config-ospf-1-area-0.0.0.100)#network 3.3.3.3 0.0.0.0
huawei(config-ospf-1-area-0.0.0.100)#return
```

Step 5 Configure a PWE3 outer tunnel.

Set the tunnel ID to 10 and the encapsulation protocol of the tunnel interface at the data link layer to MPLS IP.

```
huawei(config)#interface tunnel 10
huawei(config-if-tunnel10)#tunnel-protocol mpls ip
```

Set the destination IP address of the tunnel to the LSR ID of the PTN 9.9.9.9.

```
huawei(config-if-tunnel10)#destination 9.9.9.9
huawei(config-if-tunnel10)#quit
```

Step 6 Configure the tunnel policy.

Set the policy name to **ip_policy**.

Copyright © Huawei Technologies Co., Ltd.

```
huawei(config)#tunnel-policy ip_policy
Info: New tunnel-policy is configured.
huawei(config-tunnel-policy-ip_policy)#tunnel select-seq ip load-balance-number 1
huawei(config-tunnel-policy-ip_policy)#quit
```

Step 7 Configure PW parameters.

1. Create PW 2 and enter the PW parameter mode.
   ```
   huawei(config)#pw-para 2
   ```
2. Configure the loopback interface IP address of the remote PTN device.

   Set the loopback interface IP address to 9.9.9.9.
   ```
   huawei(config-pw-para-2)#peer-address 9.9.9.9
   ```
3. Set the PW type to TDM SAToP E1.
   ```
   huawei(config-pw-para-2)#pw-type tdm satop e1
   ```
4. Configure the PW load time.

   Set the load time to 125 μs.
   ```
   huawei(config-pw-para-2)#tdm-load-time satop e1 loadtime 125
   ```
5. Enable RTP. After RTP is enabled, PW packets of the TDM type contain the RTP control header. By default, RTP is disabled.

   NOTE

   The RTP configuration must be the same as that on the PTN.
   ```
   huawei(config-pw-para-2)#rtp-header
   ```
6. (Optional) Configure the jitter buffer size. The jitter buffer can effectively prevent jitter and latency. Only PW of the TDM type support the jitter buffer configuration. By default, the jitter buffer size is 2000 μs.

   NOTE

   The value range of the jitter buffer size is 500-32000 and the value must be an integer multiple of 125. Configure this value according to actual conditions. In this example, the jitter buffer size is set to 2500 μs.
   ```
   huawei(config-pw-para-2)#jitter-buffer buffer-size 2500
   ```
7. Configure the PW to support the control word.
   ```
   huawei(config-pw-para-2)#control-word
   ```
8. Enable virtual circuit connectivity verification (VCCV).
   ```
   huawei(config-pw-para-2)#vccv cc cw alert ttl cv lsp-ping
   ```
9. Configure the tunnel policy used by the PW parameters.

   Set the tunnel policy name to **ip-policy**.
   ```
   huawei(config-pw-para-2)#tnl-policy ip_policy
   huawei(config-pw-para-2)#quit
   ```

Step 8 Create a TDM connection.

Set the TDM connection ID to 1, type to PWE3, and ID of the E1 port on the H802EDTB board to 0/3/1.

```
huawei(config)#tdm-connect connectid 1 tdm pwe3-uplink 0/3 e1 0/3/1
```

Step 9 Bind the TDM connection to the PW to create the PW service of the TDM type.

Bind TDM connection 1 to PW2.
```
huawei(config)#pw-ac-binding tdm 1 pw 2
```

Step 10 Confirm that the PW is in the normal state.

On the OLT, run the **display pw** or **display pw-ac-binding** command to query the PW status. Confirm that the PW state is normal (**up**).

Copyright © Huawei Technologies Co., Ltd.

```
huawei(config)#display pw-ac-binding tdm 1
  Total : 1  (Up/Down :    1/0           Static/LDP :    0/1)
  ------------------------------------------------------------------------------
  TDM              PW         PW    PROTO  RECEIVE TRNS    PW
  ID               ID         STATE TYPE   LABEL   LABEL   INDEX
  ------------------------------------------------------------------------------
   1               2          up    LDP    ---     ---     2
  ------------------------------------------------------------------------------
  Note  : F--Frame, S--Slot, P--Port
          *: Secondary
```

Step 11 Configure clock synchronization on the E1 port.

Configure the recovery clock source of the H802EDTB board. In the recovery clock mode, the receive end recovers the clock of the transmit end according to the average arrival rate of the received SAToP packets. In this example, clock signals are extracted from PW2 to serve as the recovery clock of a board.

```
huawei(config)#interface edt 0/3
huawei(config-edt-0/3)#adapt-clock-source clock-source 0 2
```

Configure the Tx clock of E1 port 0/3/1 on the H802EDTB board as the network-side clock. That is, configure the clock recovered from a TDM PW as the Tx clock of a port, implementing voice service synchronization.

```
huawei(config-edt-0/3)#clock-work 1 net
```

----End

Result

After a network is restructured, the long-term bit error ratio and latency meet the requirements for actual applications, the Nx64k private line service or ISDN PRI PBX service runs normally, and the operation method for end users is not changed.

Configuration File

```
interface loopback 0
ip address 3.3.3.3 32
quit
mpls lsr-id 3.3.3.3
mpls
lsp-trigger host
quit
mpls l2vpn
mpls ldp
quit
vlan 4001 smart
port vlan 4001 0/19/0
mpls vlan 4001
interface vlanif 4001
ip address 10.50.50.50 24
mpls
mpls ldp
quit
ospf 1
area 100
network 10.50.50.0 0.0.0.255
network 3.3.3.3 0.0.0.0
return
interface tunnel 10
tunnel-protocol mpls ip
destination 9.9.9.9
quit
```


Copyright © Huawei Technologies Co., Ltd.

```
tunnel-policy ip_policy
tunnel select-seq ip load-balance-number 1
quit
pw-para 2
peer-address 9.9.9.9
pw-type tdm satop e1
tdm-load-time satop e1 loadtime 125
rtp-header
jitter-buffer buffer-size 2500
control-word
vccv cc cw alert ttl cv lsp-ping
tnl-policy ip_policy
quit
tdm-connect connectid 1 tdm pwe3-uplink 0/3 e1 0/3/1
pw-ac-binding tdm 1 pw 2
interface edt 0/3
adapt-clock-source clock-source 0 2
clock-work 1 net
```

4.3.5 Example: Configuring the TDM PWE3 to Emulate TDM Services on the MPLS Network

The MA5600T/MA5603T/MA5608T supports the SAToP encapsulation for non-frame E1 signals and implements the TDM PWE3 emulation service after MPLS-encapsulating the signals. In this way, the MA5600T/MA5603T/MA5608T provides emulated TDM private line service over the MPLS network.

Service Requirements

- To make full use of legacy TDM line and equipment, and replace legacy DDN network and ISDN PRI PBX convergence network.
- To perform MPLS over IP encapsulation on the E1 data aggregated by the Nx64k private line and ISDN PRI PBX, and transmit the data upstream as MPLS packets to the DDN network or SDH network.

Prerequisite

- The H802EDTB board and SPUB board are installed and work in the normal state.
- The working mode of the H802EDTB board is set to SAToP by running the **board workmode** command.
- A static route or dynamic route is successfully configured on each device over the network so that the IP routes between LSRs are reachable.

Context

The implementation process of TDM PWE3 is as follows:

1. The data of the Nx64k private line service or ISDN PRI PBX service is converged and then transmitted to the H802EDTB board of the MA5600T/MA5603T/MA5608T.
2. After performing SAToP processing (adding CW control word and RTP header) on the E1 data, the H802EDTB board sends the data to the SPUB board through the control board.
3. After performing the PW and MPLS encapsulation on the packets, the SPUB board adds the ETH header to the packets, and then sends them to the control board.
4. The control board performs Layer 2 forwarding and sends the packets to the upstream port.

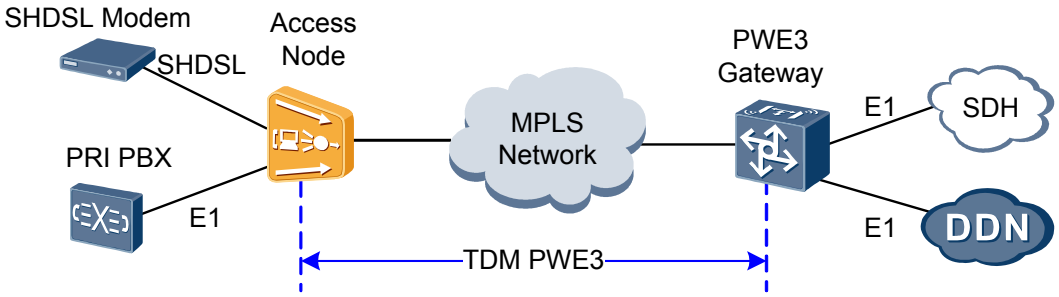
Copyright © Huawei Technologies Co., Ltd.

5. The packets are sent over the PSN network to the peer PWE3 gateway (such as the PTN).
6. The PWE3 gateway restores the E1 signals from the packets and then sends them to the DDN network or SDH network.

Networking

Figure 4-7 shows an example network of TDM PWE3 (MPLS-based).

Figure 4-7 Example network of TDM PWE3 (MPLS-based)



Data Plan

Table 4-8 lists the data plan for configuring TDM PWE3 (MPLS-based).

Table 4-8 Data plan for configuring TDM PWE3 (MPLS-based)

Parameter	Data
H802EDTB board	Board slot: 0/4 E1 port: 0/4/5
SPUB board	Board slot: 0/5
MPLS	VLAN for MPLS forwarding: 4001 IP address of VLAN interface 4001: 10.50.50.50/24 MPLS LSR ID: 3.3.3.3 Global MPLS LDP: enabled MPLS LDP for VLANIF 4001: enabled MPLS Layer 2 VPN: enabled

Copyright © Huawei Technologies Co., Ltd.

Parameter	Data
PW parameters	PW ID: 3 Peer IP address: 10.10.10.10 PW type: TDM SAToP E1 PW load time: 125 μs Jitter buffer size: 2500 μs Control word: enabled RTP: enabled VCCV: enabled
Tx clock of the E1 port	Network clock, recovered from PW 3

Procedure

Step 1 Configure a loopback interface.

Set the ID of the loopback interface to 0 and its IP address to 3.3.3.3/32.

```
huawei(config)#interface loopback 0
huawei(config-if-loopback0)#ip address 3.3.3.3 32
huawei(config-if-loopback0)#quit
```

Step 2 Enable basic MPLS functions.

Set the IP address of loopback interface 0 as the LSR ID.

```
huawei(config)#mpls lsr-id 3.3.3.3
```

Enable global MPLS.

```
huawei(config)#mpls
huawei(config-mpls)#lsp-trigger host  //set up an LSP by triggering the LDP through
the host address
huawei(config-mpls)#quit
```

Enable Layer 2 VPN.

```
huawei(config)#mpls l2vpn
```

Enable global LDP.

```
huawei(config)#mpls ldp
huawei(config-mpls-ldp)#quit
```

NOTE

- Only one session can exist between two LSRs and a local LDP session takes priority over a remote LDP session. To simplify the configuration, assume that the MA5600T/MA5603T/MA5608T is directly connected to the PTN. Hence, you need to enable only the LDP function (the local LDP session is automatically set up after the LDP function is enabled).
- If the MA5600T/MA5603T/MA5608T is not directly connected to the PTN, after the LDP function is enabled, run the **mpls ldp remote-peer** command to create an LDP remote peer and then enter the remote peer mode. Then, run the **remote-ip***ip-addr* command to specify the ID of the remote LSR.
- For detailed configurations, see Configuring the LDP LSP.

Copyright © Huawei Technologies Co., Ltd.

Step 3 Configure a VLAN and enable MPLS for the VLAN and the VLAN interface.

Add VLAN 4001 for forwarding MPLS packets and add an upstream port to it.

```
huawei(config)#vlan 4001 smart
huawei(config)#port vlan 4001 0/19/0
```

Enable MPLS for VLAN 4001.

```
huawei(config)#mpls vlan 4001
```

Set the IP address of VLAN interface 4001 to 10.50.50.50/24 and enable MPLS LDP for the VLAN interface.

```
huawei(config)#interface vlanif 4001
huawei(config-if-vlanif4001)#ip address 10.50.50.50 24
huawei(config-if-vlanif4001)#mpls
huawei(config-if-vlanif4001)#mpls ldp
huawei(config-if-vlanif4001)#quit
```

Step 4 Configure a route.

PWE3 has no special requirements for the routing policy. A static route, or dynamic RIP, or OSPF route can be configured. An OSPF dynamic route is recommended because OSPF supports MPLS RSVP-TE extension.

Set the OSPF process ID to 100 and OSPF area ID to 1. In addition, configure the interfaces (VLAN interface and loopback interface) that run OSPF and configure the areas of the interfaces.

```
huawei(config)#ospf 1
huawei(config-ospf-1)#area 100
huawei(config-ospf-1-area-0.0.0.100)#network 10.50.50.0 0.0.0.255
huawei(config-ospf-1-area-0.0.0.100)#network 3.3.3.3 0.0.0.0
huawei(config-ospf-1-area-0.0.0.100)#return
```

Step 5 Configure PW parameters.

1. Create PW 3 and enter the PW parameter mode.
   ```
   huawei(config)#pw-para 3
   ```
2. Configure the loopback interface IP address of the remote PTN device in the PW.

   Set the loopback interface IP address to 10.10.10.10.
   ```
   huawei(config-pw-para-3)#peer-address 10.10.10.10
   ```
3. Set the PW type to TDM SAToP E1.
   ```
   huawei(config-pw-para-3)#pw-type tdm satop e1
   ```
4. Configure the PW load time.

   Set the load time to 125 μs.
   ```
   huawei(config-pw-para-3)#tdm-load-time satop e1 loadtime 125
   ```
5. (Optional) Enable RTP. After RTP is enabled, PW packets of the TDM type contain the RTP control header. By default, RTP is disabled.

   NOTE

   The RTP configuration must be the same as that on the PTN.
   ```
   huawei(config-pw-para-3)#rtp-header
   ```
6. (Optional) Configure the jitter buffer size. The jitter buffer can effectively prevent jitter and delay. Only PW parameters of the TDM type support the jitter buffer configuration. By default, the jitter buffer size is 2000 μs.

Copyright © Huawei Technologies Co., Ltd.

NOTE

The value range of the jitter buffer is 500-32000 and the value must be an integer multiple of 125. You can configure this value according to actual conditions. In this example, the jitter buffer size is set to 2500 μs.

```
huawei(config-pw-para-3)#jitter-buffer buffer-size 2500
```

7. Configure the PW parameter to support the control word.
```
huawei(config-pw-para-3)#control-word
```
8. Enable virtual circuit connectivity verification (VCCV).
```
huawei(config-pw-para-3)#vccv cc cw alert ttl cv lsp-ping
```

Step 6 Create a TDM connection.

Set TDM connection ID to 2, type to PWE3, and ID of the E1 port of the H802EDTB board to 0/4/5.

```
huawei(config)#tdm-connect connectid 2 tdm pwe3-uplink 0/4 e1 0/4/5
```

Step 7 Bind the TDM connection to the PW to create the PW service of the TDM type.

Bind TDM connection 2 to PW 3.

```
huawei(config)#pw-ac-binding tdm 2 pw 3
```

Step 8 Confirm that the PW is in the normal state.

On the OLT, run the **display pw** or **display pw-ac-binding** command to query the PW status. Confirm that the PW state is normal (**up**).

```
huawei(config)#display pw-ac-binding tdm 2
  Total : 1  (Up/Down :    1/0           Static/LDP :    0/1)
  ------------------------------------------------------------------------------
  TDM              PW         PW    PROTO  RECEIVE TRNS    PW
  ID               ID         STATE TYPE   LABEL   LABEL   INDEX
  ------------------------------------------------------------------------------
   2               3          up    LDP    ---     ---     3
  ------------------------------------------------------------------------------
  Note  : F--Frame, S--Slot, P--Port
          *: Secondary
```

Step 9 Configure clock synchronization on the E1 port.

Configure the recovery clock source of the H802EDTB board. In the recovery clock mode, the receive end recovers the clock of the transmit end according to the average arrival rate of the received SAToP packets. In this example, clock signals are extracted from PW 3 to serve as the recovery clock of a board.

```
huawei(config)#interface edt 0/4
huawei(config-edt-0/4)#adapt-clock-source clock-source 0 3
```

Configure the Tx clock of E1 port 0/4/5 on the H802EDTB board as the network-side clock. That is, configure the clock recovered from a TDM PW as the Tx clock of a port, implementing voice service synchronization.

```
huawei(config-edt-0/4)#clock-work 5 net
```

----End

Result

After a network is restructured, the long-term bit error ratio and latency meet the requirements for actual applications, the Nx64k private line service or ISDN PRI PBX service runs normally, and the operation method for end users is not changed.

Copyright © Huawei Technologies Co., Ltd.

Configuration File

```
interface loopback 0
ip address 3.3.3.3 32
quit
mpls lsr-id 3.3.3.3
mpls
lsp-trigger host
quit
mpls l2vpn
mpls ldp
quit
vlan 4001 smart
port vlan 4001 0/19/0
mpls vlan 4001
interface vlanif 4001
ip address 10.50.50.50 24
mpls
mpls ldp
quit
ospf 1
area 100
network 10.50.50.0 0.0.0.255
network 3.3.3.3 0.0.0.0
return
pw-para 3
peer-address 10.10.10.10
pw-type tdm satop e1
tdm-load-time satop e1 loadtime 125
rtp-header
jitter-buffer buffer-size 2500
control-word
vccv cc cw alert ttl cv lsp-ping
tnl-policy ip_policy
quit
tdm-connect connectid 1 tdm pwe3-uplink 0/4 e1 0/4/5
pw-ac-binding tdm 2 pw 3
interface edt 0/4
adapt-clock-source clock-source 0 3
clock-work 5 net
```

4.4 Configuration Example of TDM SHDSL for Transparently Transmitting the Narrowband Data Private Line Service

The TDM SHDSL extends the access distance. With the TDM SHDSL, the MA5600T/MA5603T/MA5608T transparently transmits user-side configuration data to the digital data network (DDN). In this way, the twisted pair can be fully used and the E1 line deployment expense decreases.

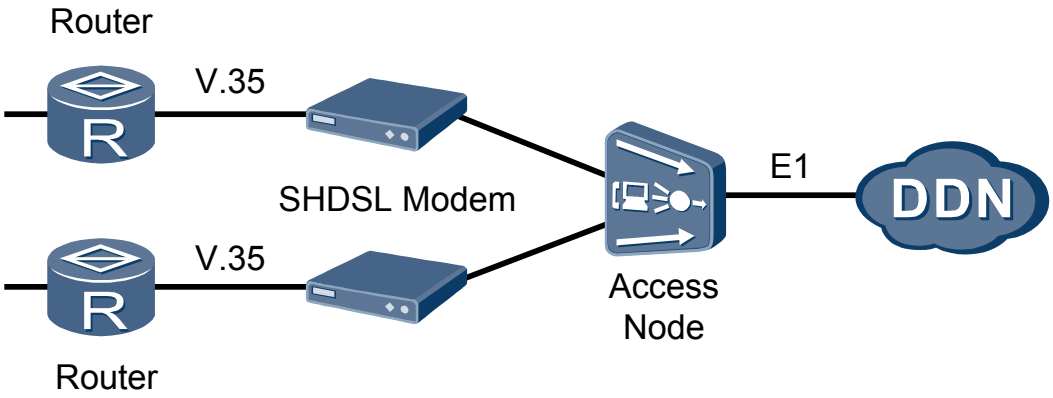
Service Requirements

- Use the existing rich twisted pair resources for long-distance transmission, extending the DDN node.
- The user-side configuration data is transparently transmitted on the MA5600T/MA5603T/MA5608T.

The following figure shows an example network of TDM SHDSL for transparently transmitting the narrowband data private line service.

Copyright © Huawei Technologies Co., Ltd.

Figure 4-8 Example network of TDM SHDSL for transparently transmitting the narrowband data private line service



Data Plan

The following table lists the data plan for configuring TDM SHDSL for transparently transmitting the narrowband data private line service.

Table 4-9 Data plan for configuring TDM SHDSL for transparently transmitting the narrowband data private line service

Item	Data
EDTB board	If the entire board is used for transparently transmitting the narrowband data private line service: ● Slot ID: 0/3 ● Board working mode: voice ● Board working sub-mode: transparent mode If a port is used for transparently transmitting the narrowband data private line service: ● Port ID: 0/3/0 ● Board working mode: voice ● Board working sub-mode: service ● Port working mode: transparent mode

Prerequisite

- The H802EDTB board must be in position and must work in the normal state.
- An SHDSL modem must be correctly connected and the SHDSL port(s) must be activated. For details, see Configuring an SHDSL Port.

Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 (Optional) Configure the working mode of the board.

Configure the working mode of the board to voice.

NOTE

The working sub-mode of the board can be configured only when the working mode of the board is configured to voice. By default, the working mode of the board is voice.

```
huawei(config)#interface edt 0/3
huawei(config-edt-0/3)#board workmode voice
```

Step 2 Configure the working sub-mode of the board according to service requirements.

- If the entire board is used for transparently transmitting the narrowband data private line service, configure the working sub-mode of the board to **transparent**.
  ```
  huawei(config-edt-0/3)#runmode transparent
  huawei(config-edt-0/3)#quit
  ```
- If a specified port is used for transparently transmitting the narrowband data private line service, configure the working sub-mode of the board to **service** and the running mode of the port to **transparent**.
  ```
  huawei(config-edt-0/3)#runmode service
  huawei(config-edt-0/3)#e1port runmode 0 transparent
  huawei(config-edt-0/3)#quit
  ```

NOTE

- Before changing the service mode to transparent mode, make sure that no service is configured for the board.
- In the transparent mode, the E1 ports and SHDSL ports are in one-to-one mapping, that is, ports 0-15 map ports 16-31 one by one.

Step 3 Save the data.

```
huawei(config)#save
```

----End

Result

The user can normally access the DDN network by using the MA5600T/MA5603T/MA5608T.

Configuration File

If the entire board is used for transparently transmitting the narrowband data private line service:

```
interface edt 0/3
board workmode voice
runmode transparent
quit
save
```

If E1 port 0 is used for transparently transmitting the narrowband data private line service:

```
interface edt 0/3
board workmode voice
runmode service
e1port runmode 0 transparent
quit
save
```


Copyright © Huawei Technologies Co., Ltd.

4.5 Configuration Example of the Private Line Service Leasing E1 Timeslots

Leasing an entire E1 line is expensive and also a waste of the bandwidth resources. The private line service leasing E1 timeslots can meet the requirement leasing a part of an E1 line. With this service, users are assigned specific timeslots of an E1 line, and therefore can share the bandwidth of the E1 line, hence saving the E1 line lease expense.

Prerequisites

- The H802EDTB board must be in position and must work in the normal state.
- An SHDSL modem must be correctly connected and the SHDSL port must be activated.

Context

The E1 private line service is mainly used in point-to-point (P2P) data exchange industries that do not require immediate data exchange, such as finance, government, and enterprise. These data exchange services do not need high bandwidth but have rigorous requirements on quality, such as error code, delay, and packet loss. Leasing an entire E1 line is expensive and also a waste of the bandwidth resources. The private line service leasing E1 timeslots can reduce costs and improve bandwidth usage, which provides rates ranging from 64 kbit/s to 2 Mbit/s.

In this case, pay attention to the signaling mode of the E1 port. The signaling mode is set to be common channel signaling (CCS) in general, which must be the same as that set on the peer device in the digital data network (DDN).

- CCS: frame format, in this mode, timeslot 0 is used to send frame synchronization information and the other 31 timeslots are used to send valid data.

Service Requirements

- Use the existing rich twisted pair resources for long-distance transmission, extending the DDN node.
- The carrier does not need to deploy the new E1 line, which saves the deployment cost. The user leases only one or more timeslots of the E1 line to save the lease expense.

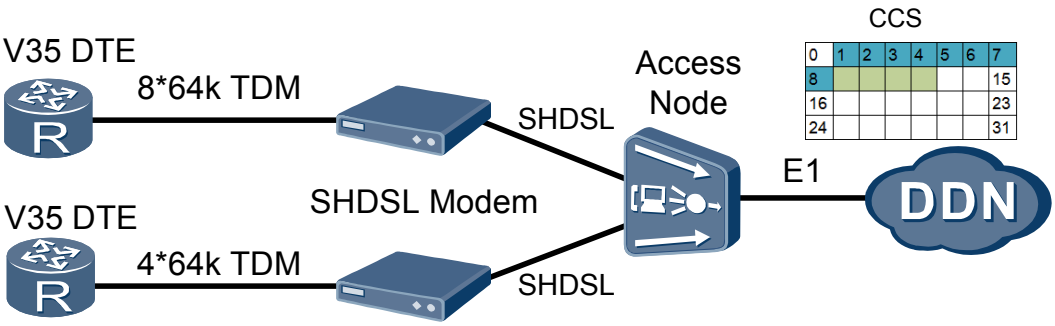
Networking

Figure 4-9 shows an example network of the private line service leasing E1 timeslots.

The user end is connected to an SHDSL modem through a data terminal equipment (DTE) that supports V.35 port, and then connected to the EDTB board of the MA5600T/MA5603T/MA5608T through the TDM SHDSL port provided by the modem. By establishing internal SPCs between different timeslots of the E1 and SHDSL ports, the EDTB board multiplexes timeslot channels of different lines to the same E1 upstream port, implementing convergence of multiple Nx64 kbit/s channels to the E1 port and saving E1 resources.

Copyright © Huawei Technologies Co., Ltd.

Figure 4-9 Example network of the private line service leasing E1 timeslots



Data Plan

Table 4-10 uses two-channel TDM aggregation (8*64 kbit/s and 4*64 kbit/s) as an example to describe the data plan in CCS mode.

Table 4-10 Data plan for configuring the private line service leasing E1 timeslots

Item	Data
EDTB board	Working mode: voice Working sub-mode: service mode Clock source: E1 line clock
E1 port	Upstream port ID: 0/3/0 Line coding mode: HDB3 (default) Port impedance: 75 ohms (default) Port signaling mode: CCS

Copyright © Huawei Technologies Co., Ltd.

Item	Data
SHDSL port	Port IDs: 0/3/16 and 0/3/17 Port signaling mode: unframe Line profile ID of the port: 2 ● Rate: 512 kbit/s ● Channel mode: TDM ● Data frame type: V35 ● Clock mode: system clock ● Other parameters: default values ● Bound to port 0/3/16 Line profile ID of the port: 3. ● Rate: 256 kbit/s ● Channel mode: TDM ● Data frame type: V35 ● Clock mode: system clock ● Other parameters: default values ● Bound to port 0/3/17
Internal SPC	Establish internal SPCs between B channels 0-7 of SHDSL port 0/3/16 and timeslots 1-8 of E1 port 0/3/0. Establish internal SPCs between B channels 0-3 of SHDSL port 0/3/17 and timeslots 9-12 of E1 port 0/3/0. **NOTE** In CCS mode, timeslot 0 of the E1 port is used to send the frame locating information but is not used to send data. Therefore, it cannot be used for internal semi-permanent connection (SPC).

Procedure

Step 1 Configure the working mode and clock source of the EDTB board.

Configure the working mode of the board to voice, working sub-mode to service, and clock source to E1 line clock.

NOTE

To configure the private line service leasing timeslots, the working mode of the board must be configured to voice and the sub-mode must be configured to service.

```
huawei(config)#interface edt 0/3
huawei(config-edt-0/3)#board workmode voice
huawei(config-edt-0/3)#runmode service
huawei(config-edt-0/3)#set clockmode line 0
```

Step 2 Configure the attributes of the SHDSL port.

1. Set the signaling mode of the SHDSL port to **unframe**.

Copyright © Huawei Technologies Co., Ltd.

```
huawei(config-edt-0/3)#shdslport signal 16 unframe
huawei(config-edt-0/3)#shdslport signal 17 unframe
huawei(config-edt-0/3)#quit
```

2. Configure the line profiles of the SHDSL port.

   Set line profile IDs to **2** and **3** with rates **512 kbit/s** and **256 kbit/s** respectively. Set the channel mode to **TDM**, data frame type to **V35**, and clock mode to system clock. Other parameters use default values.

   NOTE

   It is recommended that you set the rates on line profiles to be the same as those set on the SHDSL modem to ensure that modems are normally activated.

   The following uses adding line profile 2 as an example:

```
huawei(config)#shdsl line-profile add 2
  Start adding
profile
  During inputting,press 'Q' to quit,then settings at this time will be
ignored
  Do you want to name the profile (y/n)
[n]:n
> G.SHDSL data path mode(1--3 1--ATM;2--PTM;3--TDM)[1]:
3
> G.SHDSL interface mode of line (1--two wire;2--four wire;3--six wire;4--
eight
wire)
[1]:
> Do you use the default data to create a line profile?(y/n)
[y]:n
> G.SHDSL minimum line
rate
  (Value must be multiple of 64,except 2312kbps and
3848kbps,
  192~5696,2312,3848 kbps)[2048]:
512
> G.SHDSL maximum line
rate
  (Value must be multiple of 64,except 2312kbps and
3848kbps,
  512~5696,2312,3848 kbps)[2048]:
512
> Power spectral density mode (1--symmetric;2--asymmetric)
[1]:
> Transmission mode (1--G.991.2 Annex A/F;2--G.991.2 Annex B/
G;
  3--All)
[3]:
> Remote enable (1--enabled;2--disabled)
[1]:
> Probe enable (1--disabled;2--enabled)
[1]:
> Modulation mode(1--TCPAM16;2--TCPAM32;3--auto)
[3]:
> Performance statistic mode(1--auto;2--absolute;3--delta)
[1]:
> G.SHDSL data frame type(1--E1;2--V35)[1]:
2
> G.SHDSL data clock align(1--synchronization 2--asynchronism)
[1]:
> Clock mode(1--freeRun 2--system)[1]:
2
> Do you config the target SNR margin?(y/n)
[n]:n
  Add profile 2 successfully
```


Copyright © Huawei Technologies Co., Ltd.

3. Bind the line profile and activate the SHDSL port.

```
huawei(config)#interface shl 0/3
huawei(config-shl-0/3)#deactivate all
huawei(config-shl-0/3)#activate 16 2
huawei(config-shl-0/3)#activate 17 3
uawei(config-shl-0/3)#quit
```

Step 3 Configure the attributes of the upstream E1 port.

Set the signaling mode of the E1 port to CCS.

```
huawei(config)#interface edt 0/3
huawei(config-edt-0/3)#e1port signal 0 ccs
huawei(config-edt-0/3)#quit
```

Step 4 Configure internal SPCs.

Create one-to-one mapping from eight B channelsof SHDSL port 0/3/16 to eight timeslots of E1 port 0/3/0; create one-to-one mapping from four B channels of SHDSL port 0/3/17 to four timeslots of E1 port 0/3/0. This implements the convergence of (8+4) x 64 kbit/s channels.

NOTE

In CCS mode, timeslot 0 of the E1 port is used to send the frame locating information but is not used to send data. Therefore, it cannot be used for internal SPC.

```
huawei(config)#spc
huawei(config-spc)#anspc add start 0/3/16/0 end 0/3/0/1 apptype normal channelnum
8
huawei(config-spc)#anspc add start 0/3/17/0 end 0/3/0/9 apptype normal channelnum
4
```

Step 5 Query the status of the internal SPCs.

```
huawei(config-spc)#display anspc from-connectid 0
{ <cr>|to-connectid<K> }:

  Command:
          display anspc from-connectid 0
------------------------------------------------------------------------------
  ConnectId               :0
  Start F/S/P/Chn         :0  /3/16/0
  End F/S/P/Chn           :0  /3/0 /1
  BChannelNum             :8
  State                   :normal
  Apptype                 :normal
  Description             :timeslot0-7_to_e1timeslot1-8
------------------------------------------------------------------------------
  ConnectId               :1
  Start F/S/P/Chn         :0  /3/17/0
  End F/S/P/Chn           :0  /3/0 /9
  BChannelNum             :4
  State                   :normal
  Apptype                 :normal
  Description             :timeslot0-3_to_e1timeslot9-12
------------------------------------------------------------------------------
```

----End

Result

- The above-mentioned users can normally access the DDN by using the leased E1 timeslots.
- The P2P data services of users are normal and no error codes are generated in a long-time service test.

Copyright © Huawei Technologies Co., Ltd.

Configuration File

```
interface edt 0/3
board workmode voice
runmode service
set clockmode line 0
shdslport signal 16 unframe
shdslport signal 17 unframe
quit
shdsl line-profile add 2
shdsl line-profile add 3
interface shl 0/3
deactive all
activate 16 2
activate 17 3
quit
interface edt 0/3

e1port signal 0 ccs
quit

spc
anspc add start 0/3/16/0 end 0/3/0/1 apptype normal channelnum 8
anspc add start 0/3/17/0 end 0/3/0/9 apptype normal channelnum 4
```


Copyright © Huawei Technologies Co., Ltd.

5 Configuration Example of MSTP Subtending Network

About This Chapter

This topic describes how to configure the integrated services on the MA5600T/MA5603T/MA5608Ts in the MSTP ring network.

5.1 MSTP Networking
This topic describes the typical networking in the MSTP mode.

5.2 MSTP Dataplan
This topic provides the data plan for the example RSTPMSTP network.

5.3 Configuring MA5600T/MA5603T/MA5608T-1
This topic describes how to configure MA5600T/MA5603T/MA5608T-1.

5.4 Configuring MA5600T/MA5603T/MA5608T-2
This topic describes how to configure MA5600T/MA5603T/MA5608T-2.

5.5 Configuring MA5600T/MA5603T/MA5608T-3
This topic describes how to configure MA5600T/MA5603T/MA5608T-3.

5.6 Configuring MA5600T/MA5603T/MA5608T-4
This topic describes how to configure MA5600T/MA5603T/MA5608T-4.

5.7 Configuring MA5600T/MA5603T/MA5608T-5
This topic describes how to configure MA5600T/MA5603T/MA5608T-5.

5.8 Verification
All services configured on all DSLAMs run in the normal state.

Copyright © Huawei Technologies Co., Ltd.

5.1 MSTP Networking

This topic describes the typical networking in the MSTP mode.

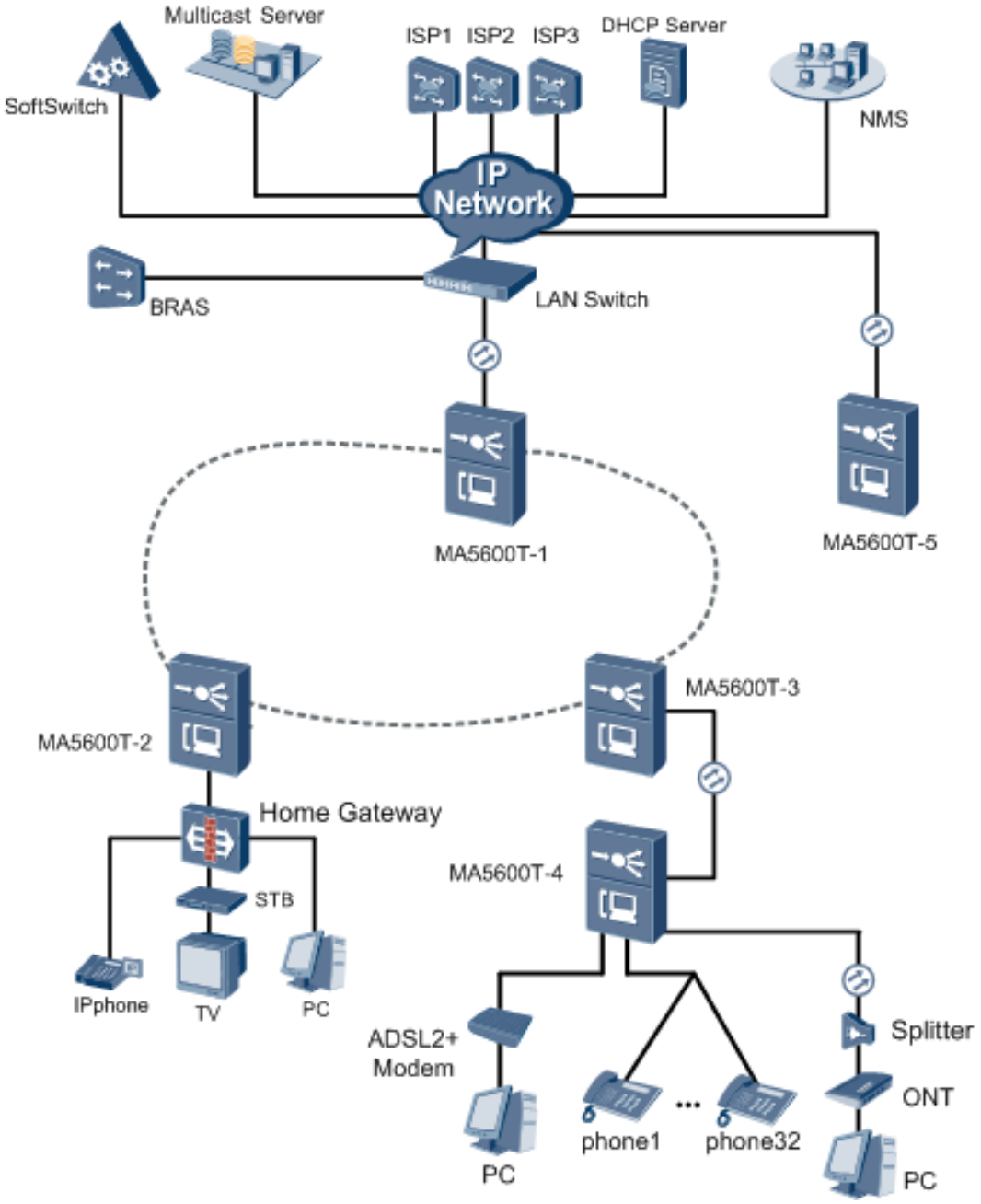
Three MA5600T/MA5603T/MA5608Ts (MA5600T/MA5603T/MA5608T-1, MA5600T/MA5603T/MA5608T-2, and MA5600T/MA5603T/MA5608T-3) form an MSTP ring network.

- MA5600T/MA5603T/MA5608T-1 is connected to the IP network.
- MA5600T/MA5603T/MA5608T-2 is connected to the home gateway at the user end through the xDSL service board, providing the Internet, voice, and IPTV services concurrently.
- MA5600T/MA5603T/MA5608T-3, through whose GE port, is subtended with MA5600T/MA5603T/MA5608T-4.
- MA5600T/MA5603T/MA5608T-1 works with MA5600T/MA5603T/MA5608T-5 to provide the QinQ service through the IP network.

Figure 5-1 shows an example MSTP network of the MA5600T/MA5603T/MA5608T.

Copyright © Huawei Technologies Co., Ltd.

Figure 5-1 Example MSTP network of the MA5600T/MA5603T/MA5608T



5.2 MSTP Dataplan

This topic provides the data plan for the example RSTPMSTP network.

Table 5-1 provides the service and the data plan for the example network of the MA5600T/MA5603T/MA5608T.

Copyright © Huawei Technologies Co., Ltd.

Table 5-1 Data plan for the example RSTPMSTP network

Item	MA5600T/ MA5603T/ MA5608T-1	MA5600T/ MA5603T/ MA5608T-2	MA5600T/ MA5603T/ MA5608T -3	MA5600T/ MA5603T/ MA5608T-4	MA5600T/ MA5603T/ MA5608T-5
Service	● ADSL2+ service ● SHDSL service ● GPON service ● POTS service ● QinQ private line service (interoperate with MA5600T / MA5603T / MA5608T -5) ● Multicast service	● ADSL2+ service ● SHDSL service ● POTS service ● Stacking wholesale service ● Triple play service (multiple PVCs for multiple services) ● Multicast service	● ADSL2+ service ● SHDSL service ● GPON service	● ADSL2+ service ● SHDSL service ● POTS service ● GPON service ● Multicast service	● VDSL2 service ● QinQ private line service (interoperate with MA5600T/ MA5603T/ MA5608T-1)
Inband NMS address	10.10.1.2 255.255.255.0 Gateway: 10.10.1.1/24	10.10.1.3 255.255.255.0 Gateway: 10.10.1.1/24	10.10.1.4 255.255.255.0 Gateway: 10.10.1.1/24	10.10.1.5 255.255.255.0 Gateway: 10.10.1.1/24	10.10.1.6 255.255.255.0 Gateway: 10.10.1.1/24
GE port of the GIU board	Upstream: 0/20/0 RSTP: 0/19/0-0/19/1	Upstream: 0/19/0-0/19/1	Upstream: 0/19/0-0/19/1 RSTP: 0/20/0	Upstream: 0/19/0	Upstream: 0/19/0

Copyright © Huawei Technologies Co., Ltd.

Item	MA5600T/ MA5603T/ MA5608T-1	MA5600T/ MA5603T/ MA5608T-2	MA5600T/ MA5603T/ MA5608T -3	MA5600T/ MA5603T/ MA5608T-4	MA5600T/ MA5603T/ MA5608T-5
VLAN	NMS: 10 QinQ: 50 Multicast: 100 ADSL2+: 1000-1031 (uses the VLAN authentication) SHDSL: 1300-1315 (uses the VLAN authentication) GPON: 1510 (the ONT uses the SN + password authentication) POTS: 1600 (uses the H. 248 protocol)	NMS: 10 Multicast: 100 Stacking: 60-62 (inner stacking: 111-113) Triple play: 100-102 ADSL2+: 2020 (uses the PPPoE authentication) SHDSL: 3020 (uses the PPPoE authentication) POTS: 1600 (uses the H.248 protocol)	NMS: 10 ADSL2+: 2030 (uses the PPPoE authentication) SHDSL: 3030 (uses the PPPoE authentication) GPON: 1530 (the ONT uses the SN + password authentication)	NMS: 10 Multicast: 100 ADSL2+: 2040 (uses the PPPoE authentication) SHDSL: 3040 (uses the PPPoE authentication) GPON: 1540 (the ONT uses the SN + password authentication) POTS: 1600 (uses the H. 248 protocol)	NMS: 10 QinQ: 50 VDSL2: 1800 (uses the PPPoE authentication)
Slot	ADSL2+: 0/2 SHDSL: 0/5 GPON: 0/18 POTS: 0/3 QinQ: 0/5/31 Multicast: 0/2/2, 0/2/3	ADSL2+: 0/2 SHDSL: 0/5 POTS: 0/3 Stacking: 0/2/0-10 (maps VLAN 60, ISP1) 0/2/11-20 (maps VLAN 61, ISP2) 0/2/21-30 (maps VLAN 62, ISP3) Triple Play: 0/2/31	ADSL2+: 0/2 SHDSL: 0/5 GPON: 0/18	ADSL2+: 0/2 SHDSL: 0/5 GPON: 0/18 POTS: 0/3 Multicast: 0/2/2, 0/2/3	SHDSL: 0/5 VDSL: 0/2 QinQ: 0/5/15

Copyright © Huawei Technologies Co., Ltd.

Item	MA5600T/ MA5603T/ MA5608T-1	MA5600T/ MA5603T/ MA5608T-2	MA5600T/ MA5603T/ MA5608T-3	MA5600T/ MA5603T/ MA5608T-4	MA5600T/ MA5603T/ MA5608T-5
User PVC	PVC VPI/VCI of all users: 0/35	VPI/VCI of the triple play: ● Video service: 0/35 ● Internet service: 0/36 ● Voice service: 0/37	PVC VPI/ VCI of all users: 0/35	PVC VPI/ VCI of all users: 0/35	PVC VPI/ VCI of all users: 0/35
POTS service	MGC IP address: 10.30.80.65/24 Media/Signaling IP address of the MG interface: 10.176.6.33/24 Default media gateway of the MG interface: 10.176.6.62/24 IP address of the VLAN: 10.176.6.33/24 MG interface attributes: index is 0, supported protocol is H.248, coding type is text, signaling port number is 2944, port number of the active MGC is 2944, and transmission mode is UDP.				
NMS host	2.2.2.2 and 2.2.2.3				
Log host	3.3.3.3 and 3.3.4.3				
Time server	4.4.4.4 and 4.4.4.5				
Multicast server	10.10.10.10				
EMU	AC PS4845 power monitoring, fan monitoring				
DHCP server	DHCP server1: 10.1.1.2 (active) 10.1.1.3 (standby) Gateway: 10.1.1.1/24 DHCP server2: 10.4.4.2 (active) 10.4.4.3 (standby) Gateway: 10.4.4.1/24				
Upper-layer device	The upper-layer device supports the DHCP option82 function. The BRAS supports the PITP, stacking VLAN and QinQ VLAN function. The BRAS supports inner and outer VLAN tags. The VLAN ID of the traffic flow sent from the IP network to the DSLAM is 100. The upper layer device classifies the downstream traffic. Different service carries different 802.1p labels. The VLAN mapping to the DSLAM is configured in the upper-layer IP network.				

Copyright © Huawei Technologies Co., Ltd.

NOTE

- In this networking, MA5600T/MA5603T/MA5608T-1 can be replaced with a GE switch or a BRAS.
- The upstream port of MA5600T/MA5603T/MA5608T supports the port aggregation function. In the actual network planning, you can aggregate multiple ports for use.
- In this networking, the five MA5600T/MA5603T/MA5608Ts support the ADSL2+, SHDSL, VDSL2, GPON, and POTS services. You can plan the services according to your actual network conditions.

5.3 Configuring MA5600T/MA5603T/MA5608T-1

This topic describes how to configure MA5600T/MA5603T/MA5608T-1.

Procedure

Step 1 Confirm the board.

```
huawei>enable
huawei#config
huawei(config)#board confirm 0
```

Step 2 Configure the NMS.

1. Configure the IP address of the inband NMS interface.
   - Create the NMS VLAN.
     ```
     huawei(config)#vlan 10 standard
     ```
   - Add the upstream port.
     ```
     huawei(config)#port vlan 10 0/19 0-2
     ```
   - Enter the NMS VLAN interface mode.
     ```
     huawei(config)#interface vlanif 10
     ```
   - Configure the IP address of the NMS VLAN interface.
     ```
     huawei(config-if-vlanif10)#ip address 10.10.1.2 255.255.255.0
     huawei(config-if-vlanif10)#quit
     ```
2. Add the route.
   - Configure the route destined to the NMS (trap destination host).
     ```
     huawei(config)#ip route-static 2.2.2.2 255.255.255.255 10.10.1.1
     preference 1
     ```
   - Configure the route destined to the time server.
     ```
     huawei(config)#ip route-static 4.4.4.0 255.255.255.0 10.10.1.1
     preference 1
     ```
   - Configure the route destined to the log host.
     ```
     huawei(config)#ip route-static 3.3.3.0 255.255.255.0 10.10.1.1
     preference 1
     huawei(config)#ip route-static 3.3.4.0 255.255.255.0 10.10.1.1
     preference 1
     ```
3. Add the ACL rule.
   ```
   huawei(config)#acl 3050
   huawei(config-acl-adv-3050)#rule permit ip source any destination any
   huawei(config-acl-adv-3050)#rule deny ip source any destination 10.10.1.2
   0.0.0.0
   huawei(config-acl-adv-3050)#rule permit ip source 2.2.2.2 0.0.0.0
   destination 10.10.1.2 0.0.0.0
   huawei(config-acl-adv-3050)#rule permit ip source 2.2.2.3 0.0.0.0
   destination 10.10.1.2 0.0.0.0
   ```


Copyright © Huawei Technologies Co., Ltd.

```
huawei(config-acl-adv-3050)#rule permit ip source 4.4.4.4 0.0.0.0
destination 10.10.1.2 0.0.0.0
huawei(config-acl-adv-3050)#rule permit ip source 4.4.4.5 0.0.0.0
destination 10.10.1.2 0.0.0.0
huawei(config-acl-adv-3050)#rule permit ip source 3.3.3.3 0.0.0.0
destination 10.10.1.2 0.0.0.0
huawei(config-acl-adv-3050)#rule permit ip source 3.3.4.3 0.0.0.0
destination 10.10.1.2 0.0.0.0
huawei(config-acl-adv-3050)#quit
huawei(config)#packet-filter inbound ip-group 3050 port 0/19/1
huawei(config)#packet-filter inbound ip-group 3050 port 0/20/0
```

4. Configure the SNMP parameters.
   - Configure the community name and the access authority.
     ```
     huawei(config)#snmp-agent community read public
     huawei(config)#snmp-agent community write private
     ```
   - Configure the contact information.
     ```
     huawei(config)#snmp-agent sys-info contact HW-075512345678
     ```
   - Configure the device location information.
     ```
     huawei(config)#snmp-agent sys-info location Shenzhen China
     ```
   - Configure the SNMP version.

     The SNMP version must be the same as the SNMP version of the NMS. In this example, the NMS version is set as SNMP v2c.

     ```
     huawei(config)#snmp-agent sys-info version v2c
     ```
5. Enable the trap sending.
   ```
   huawei(config)#snmp-agent trap enable standard
   ```
6. Set the trap destination address.
   ```
   huawei(config)#snmp-agent target-host trap-hostname huawei address 2.2.2.2
   trap-paramsname abc
   huawei(config)#snmp-agent target-host trap-hostname huawei123 address 2.2.2.3
   trap-paramsname 123
   ```
7. Set the trap source address.
   ```
   huawei(config)#snmp-agent trap source vlanif 10
   ```

Step 3 Configure the time server.

```
huawei(config)#ntp-service unicast-server 4.4.4.4 source-interface vlanif 10
huawei(config)#ntp-service unicast-server 4.4.4.5 source-interface vlanif 10
```

Step 4 Configure the log host.

```
huawei(config)#loghost add 3.3.3.3 syslog-1
huawei(config)#loghost activate ip 3.3.3.3
huawei(config)#loghost add 3.3.4.3 syslog-2
huawei(config)#loghost activate ip 3.3.4.3
```

Step 5 Configure the EMU.

This topic uses the fan and PS4875L power supply as an example to describe how to configure the environment monitoring unit (EMU).

By default, the default slave node number of the fan EMU is 0. In this example, suppose the slave node number is 1. In this case, you need to set the DIP switch of the slave node number on the fan monitoring unit as 1.

```
huawei(config)#emu add 0 power4875l 0 0
huawei(config)#emu add 1 fan 0 1
huawei(config)#interface emu 0
huawei(config-if-power4875l-0)#power module-num 2 1 2
huawei(config-if-power4875l-0)#quit
```


Copyright © Huawei Technologies Co., Ltd.

Step 6 Configure GIU subtending

MA5600T/MA5603T/MA5608T-1 is subtended with MA5600T/MA5603T/MA5608T-2, MA5600T/MA5603T/MA5608T-3 and MA5600T/MA5603T/MA5608T-4. Therefore, subtending should be configured.

```
huawei(config)#vlan 60 to 62 standard
huawei(config)#port vlan 60 to 62 0/19 0-2
huawei(config)#vlan 101 to 102 standard
huawei(config)#port vlan 101 to 102 0/19 0-2
```

Step 7 Configure MSTP.

1. Enable the MSTP function.

```
huawei(config)#stp enable
  Change global stp state may active region configuration,it may take
several
minutes,are you sure to change global stp state? [Y/N][N]
Y
```

2. Set the MST region name.

```
huawei(config)#stp region-configuration
huawei(stp-region-configuration)#region-name hwrg
```

3. Configure MSTP instance 1.

```
huawei(stp-region-configuration)#instance 1 vlan 1 to 4094
```

4. Activate the configuration of the MST region.

```
huawei(stp-region-configuration)#active region-configuration
  STP actives region configuration, it may take several minutes,are you sure
to
active region configuration? [Y/N][N]y
```

5. Set the priority of MA5600T/MA5603T/MA5608T_1 in the instance.

```
huawei(stp-region-configuration)#quit
huawei(config)#stp instance 0 priority 0
huawei(config)#stp instance 1 priority 0
```

Step 8 Configure ADSL2+ service.

The MA5600T/MA5603T/MA5608T supports the ADSL2+ service of multiple encapsulation modes, such as IPoA, PPPoA, IPoE, and PPPoE. This topic uses the PPPoE mode as an example to describe how to configure the ADSL2+ service. For other encapsulation modes, see "**3.1 Example: Configuring the xDSL Internet Access Service**."

1. Configure the ADSL2+ line profile.

   You can configure the ADSL2+ line profile based on your requirements.

```
huawei(config)#adsl line-profile add 10
  Start adding
profile
  Press 'Q' to quit the current configuration and new configuration will
be
neglected
>  Do you want to name the profile (y/n)
[n]:
>    Transmission
mode:
>      0:
Custom
>      1: All (G.
992.1~5,T1.413,ETSI)
>      2: Full rate(G.
992.1/3/5,T1.413,ETSI)
>      3: G.DMT (G.
992.1/3/5)
```


Copyright © Huawei Technologies Co., Ltd.

```
>      4: G.HS (G.
992.1~5)
>      5: ADSL (G.
992.1~2,ETSI,T1.413)
>      6: ADSL2 & ADSL2+ (G.
992.3~5)
>    Please select (0~6)
[1]:
>  Trellis mode 1-disable 2-enable (1~2)
[2]:
>  Bit swap downstream 1-disable 2-enable (1~2)
[2]:
>  Bit swap upstream 1-disable 2-enable (1~2)
[2]:
>  Please select the form of transmit rate adaptation
downstream:
>  1-fixed, 2-adaptAtStartup, 3-adaptAtRuntime (1~3)
[2]:
>  Please select the form of transmit rate adaptation
upstream:
>  1-fixed, 2-adaptAtStartup, 3-adaptAtRuntime (1~3)
[2]:
>  Will you set SNR margin parameters? (y/n)
[n]:
>  Will you set DPBO parameters? (y/n)
[n]:
>  Will you set power management parameters? (y/n)
[n]:
>  Will you set tone blackout configuration parameter? (y/n)
[n]:
>  Will you set INM downstream parameter? (y/n)
[n]:
>  Will you set RFI notch configuration parameter? (y/n)
[n]:
>  Will you set mode-specific parameters? (y/n)
[n]:
>  Will you set network timing reference? (y/n) [n]:
  Add profile 10 successfully
```

2. Configure the ADSL2+ channel profile.

   You can configure the ADSL2+ channel profile based on your requirements.

```
huawei(config)#adsl channel-profile add 10
  Start adding
profile
  Press 'Q' to quit the current configuration and new configuration will
be
neglected
>  Do you want to name the profile (y/n)
[n]:n
>  Data path mode 1-ATM, 2-PTM, 3-Both (1~3) [3]:
1
>  Will you set the minimum impulse noise protection? (y/n)
[n]:y
>    Minimum impulse noise protection
downstream:
>    1-noProtection    2-halfSymbol      3-singleSymbol     4-
twoSymbols
>    5-threeSymbols    6-fourSymbols     7-fiveSymbols      8-
sixSymbols
>    9-sevenSymbols    10-eightSymbols   11-nineSymbols     12-
tenSymbols
>    13-elevenSymbols  14-twelveSymbols  15-thirteenSymbols 16-
fourteenSymbols
>    17-fifteenSymbols 18-
sixteenSymbols
>    Please select (1~18) [2]:
4
```


Copyright © Huawei Technologies Co., Ltd.

```
>    Minimum impulse noise protection
upstream:
>    1-noProtection    2-halfSymbol      3-singleSymbol     4-
twoSymbols
>    5-threeSymbols    6-fourSymbols     7-fiveSymbols      8-
sixSymbols
>    9-sevenSymbols    10-eightSymbols   11-nineSymbols     12-
tenSymbols
>    13-elevenSymbols  14-twelveSymbols  15-thirteenSymbols 16-
fourteenSymbols
>    17-fifteenSymbols 18-
sixteenSymbols
>    Please select (1~18) [2]:
4
>  Will you set interleaving delay parameters? (y/n)
[n]:y
>    Maximum interleaving delay downstream (0~63 ms) [16]:
24
>    Maximum interleaving delay upstream (0~63 ms) [6]:
12
>  Will you set parameters for rate? (y/n)
[n]:y
>    Minimum transmit rate downstream (32~32000 Kbps)
[32]:
>    Minimum reserved transmit rate downstream (32~32000 Kbps)
[32]:
>    Maximum transmit rate downstream (32~32000 Kbps) [24544]:
8000
>    Minimum transmit rate upstream (32~6000 Kbps)
[32]:
>    Minimum reserved transmit rate upstream (32~6000 Kbps)
[32]:
>    Maximum transmit rate upstream (32~6000 Kbps)
[1024]:
>  Will you set rate thresholds? (y/n)
[n]:
>  Will you set retransmission function (y/n)
[n]:
>  Will you set erasure decoding? (y/n) [n]:
  Add profile 10 successfully
```

3. Configure the ADSL2+ line template.

   Bind the preceding configured line profile and the channel profile together in the line template with the index of 10.

```
huawei(config)#adsl line-template add
10
  Start adding
template
  Press 'Q' to quit the current configuration and new configuration will
be
neglected
>  Do you want to name the template (y/n)
[n]:
>  Please set the line-profile index (1~128) [1]:
10
>  Will you set channel configuration parameters? (y/n)
[n]:y
>    Please set the channel number (1~2) [1]:
1
>    Channel1 configuration
parameters:
>    Please set the channel-profile index (1~128) [1]:
10
  Add template 10
successfully
```


Copyright © Huawei Technologies Co., Ltd.

4. Configure the ADSL2+ alarm profile.

   You can configure the ADSL2+ alarm profile based on your requirements. For detailed configuration, see "Configuring an ADSL2+ Alarm Template." This example adopts the default alarm profile 1 in the system.

5. Configure the ADSL2+ traffic profile.

   You can configure the ADSL2+ traffic profile by running the **traffic table ip** command based on your requirements.

   In this example, the default profile (profile 6) is used.

6. Activate the ADSL2+ port.

```
huawei(config)#interface adsl 0/2
huawei(config-if-adsl-0/2)#deactivate all
huawei(config-if-adsl-0/2)#alarm-config all 1
huawei(config-if-adsl-0/2)#activate all template-index 1
huawei(config-if-adsl-0/2)#quit
```

7. Configure the upstream port.

   - Configure the GIU board.

     The configuration of the upstream port of the GIU board should be the same as that of the peer device.

     Run the **auto-neg** command to set the port to work in the auto-negotiation mode.

     If the port does not work in the auto-negotiation mode, change to the GIU config mode and run the **speed** command to change the port rate, and run the **duplex** command to change the port duplex mode.

   - Configure the VLAN.

     The ADSL2+ users of MA5600T/MA5603T/MA5608T-1 use the VLAN authentication. In this case, the MUX VLAN is used to identify the users.

```
huawei(config)#vlan 1000 to 1031 mux
huawei(config)#port vlan 1000 to 1031 0/19 0-2
huawei(config)#port vlan 60 to 62 0/19 0-2
```

8. Add the service port.

   All ports in slot 0/3 provide the ADSL2+ service. To add service ports in batches, run the **multi-service-port** command.

```
huawei(config)#multi-service-port from-vlan 1000 port 0/2 0-31 vpi 0 vci 35 rx-cttr 6 tx-cttr 6
```

Step 9 Configure the SHDSL service.

The MA5600T/MA5603T/MA5608T supports the SHDSL service of multiple encapsulation modes, such as IPoA, PPPoA, IPoE, and PPPoE. This topic takes the PPPoE mode as an example to describe how to configure the SHDSL service. For other encapsulation modes, see "**3.1 Example: Configuring the xDSL Internet Access Service**."

1. Configure the SHDSL line profile.

   To configure the SHDSL line profile, run the **shdsl line-profile add** or **shdsl line-profile quickadd** command.

```
huawei(config)#shdsl line-profile quickadd 10 line two-wire rate 2048 2048 psd
symmetric transmission Annex-A remote disable probe disable snr-margin ds-curr 10 ds-worst
 10 us-curr 10 us-worst 10 bitmap 0x03
```


Copyright © Huawei Technologies Co., Ltd.

2. Configure the SHDSL alarm profile.

   To configure the SHDSL alarm profile, run the **shdsl alarm-profile add** command.

   In this example, the default profile (profile 1) is used.

3. Activate the SHDSL port.

```
huawei(config)#interface shl 0/5
huawei(config-if-shl-0/5)#deactivate all
huawei(config-if-shl-0/5)#alarm-config all 1
huawei(config-if-shl-0/5)#activate all 10
huawei(config-if-shl-0/5)#quit
```

4. Configure the upstream port.

   The SHDSL users of MA5600T/MA5603T/MA5608T-1 adopt the VLAN authentication. In this case, the MUX VLAN is used to identify the users.

```
huawei(config)#vlan 1300 to 1315 mux
huawei(config)#port vlan 1300 to 1315 0/19 0-2
```

5. Add the service port.

   Ports 0-14 in slot 0/5 provide the SHDSL service. To activate the ports in batches, run the **multi-service-port** command.

```
huawei(config)#multi-service-port from-vlan 1300 port 0/5 0-15 vpi 0 vci 35 rx-cttr 6 tx-cttr 6
```

Step 10 Configure the GPON service.

1. Configure the service VLAN and the upstream port.

```
huawei(config)#vlan 1510 smart
huawei(config)#port vlan 1510 0/19 0
```

2. Configure the DBA profile.

```
huawei(config)#dba-profile add profile-id 10 type1 fix 102400
```

3. Configure the alarm threshold profile.

   - When you need to configure the alarm threshold value to monitor the performance statistics of the activated ONT line, run the **gpon alarm-profile add** command to configure the GPON alarm threshold profile.
   - In the default GPON alarm threshold profile 1, all alarm thresholds are set to 0, which indicates that no alarm is reported.
   - In this example, the default alarm threshold profile is used. You do not need to configure it.

4. Configure the GPON traffic profile.

```
huawei(config)#traffic table ip index 8 cir 10240 priority 0 priority-policy tag-In-Package
```

5. Add an ONT.

   NOTE

   - You can add an ONT in two ways: run the **ont add** command to add an ONT offline or run the **ont confirm** command to confirm an ONT that is in the auto-find state.
   - You need to run the **port ont-auto-find** command in the GPON mode to enable the auto-find function of the ONT.

```
huawei(config)#interface gpon 0/18
huawei(config-if-gpon-0/18)#ont add 1 sn-auth hwhw-10101010 profile-id 2
```

   NOTE

   In this example, the ONT uses the default capability set profile 2. You can run the **ont-profile add** command to configure the capability set profile of the ONT based on your requirements.

Copyright © Huawei Technologies Co., Ltd.

6. Bind the alarm threshold profile.

```
huawei(config-if-gpon-0/18)#ont alarm-profile 1 0 profile-id 1
```

7. Bind the DBA profile.

```
huawei(config-if-gpon-0/18)#tcont bind-profile 1 0 1 profile-id 10
```

8. Divide the ONT port VLAN.

```
huawei(config-if-gpon-0/18)#ont port vlan 1 0 eth 10 0
huawei(config-if-gpon-0/18)#ont port native-vlan 1 0 eth 1 vlan 1510
```

9. Configure the GEM port.

```
huawei(config-if-gpon-0/18)#gemport add 1 gemportid 150 eth
```

10. Bind the GEM port to an ONT T-CONT.

NOTE

In the actual application, if the ONT terminal does not support the priority queue scheduling, you can use the CAR to limit the rate when binding the GEM port to the ONT T-CONT.

```
huawei(config-if-gpon-0/18)#ont gemport bind 1 0 150 1 priority-queue 3
```

11. Create the mapping between the GEM port and the service stream.

```
huawei(config-if-gpon-0/18)#ont gemport mapping 1 0 150 vlan 1510
```

12. Add the service port.

```
huawei(config-if-gpon-0/18)#quit
huawei(config)#service-port vlan 1510 gpon 0/18/0 gemport 150 multi-service
user-vlan 10 rx-cttr 5 tx-cttr 8
```

Step 11 Configure the POTS service.

1. Configure the upstream ports of the media stream and the signaling flow.

```
huawei(config)#vlan 1600 smart
huawei(config)#port vlan 1600 0/19 0
huawei(config)#interface vlanif 1600
huawei(config-if-vlanif1600)#ip address 10.176.6.33 24
huawei(config-if-vlanif1600)#quit
```

2. Configure the static route destined to the MGC.

NOTE

When the MGC and the MG are in the same network segment, you do not need to configure the static route.

```
huawei(config)#ip route-static 10.30.80.0 255.255.255.0 10.176.6.62
```

3. Configure the media IP address pool and the signaling IP address pool.

```
huawei(config)#voip
huawei(config-voip)#ip address media 10.176.6.33 10.176.6.62
huawei(config-voip)#ip address signaling 10.176.6.33
huawei(config-voip)#quit
```

4. Configure the MG interface.

Add an MG interface.

```
huawei(config)#interface h248 0
  Are you sure to add MG interface? (y/n)[n]:y
```

Configure the MG interface attributes.

```
huawei(config-if-h248-0)#if-h248 attribute mgip 10.176.6.33 mgport 2944 code
text
transfer udp primary-mgc-ip1 10.30.80.65 primary-mgc-port 2944 mg-media-ip1
10.176.6.33
```

Configure the software parameters of the MG interface (in this example, only parameter 20 is configured, and other parameters use the default values).

Copyright © Huawei Technologies Co., Ltd.

```
huawei(config-if-h248-0)#mg-software parameter 20 2
```

5. Reset the MG interface.

   NOTE

   After configuring the MG interface, you need to reset the interface to validate the configuration.

```
huawei(config-if-h248-0)#reset coldstart
  Are you sure to reset MG interface?(y/n)[n]:y
huawei(config-if-h248-0)#quit
```

6. Configure the data of PSTN user.

```
huawei(config)#esl user
huawei(config-esl-user)#mgpstnuser batadd 0/3/0 0/3/31 0 terminalid 0 telno
88660000
huawei(config-esl-user)#quit
```

Step 12 Configure the QinQ private line service.

MA5600T/MA5603T/MA5608T-1 and MA5600T/MA5603T/MA5608T-5 serve two branches of a company to provide the QinQ private line service.

1. Create VLAN 50.

```
huawei(config)#vlan 50 mux
```

2. Set VLAN 50 as QinQ VLAN.

```
huawei(config)#vlan attrib 50 q-in-q
```

3. Add the upstream port.

```
huawei(config)#port vlan 50 0/19 0-2
```

4. Add the service port.

   To add the service port, run the **service-port** command. Note that the VPI and VCI values set during the execution of the **service-port** command must be the same as those on the modem.

   The QinQ VLAN supports the PVC-priority scheduling policy only. In this case, select the profile that supports PVC-priority policy.

```
huawei(config)#traffic table ip index 7 cir off priority 0 priority-policy
local-Setting
huawei(config)#service-port vlan 50 shdsl mode atm 0/5/15 vpi 0 vci 36 rx-cttr
7 tx-cttr 7
```

Step 13 Configure the multicast service.

After the configuration, the following results should be achieved:

- Users of port 0/2/2 must be authenticated, and have rights to watch two programs and to preview one program.
- Users of port 0/2/3 do not need authenticating.

1. Configure the xDSL.

   In this example, it is unnecessary to configure the xDSL. The default line profile (profile 1002) is used.

2. Configure the VLAN.
   - Create a VLAN.
     ```
     huawei(config)#vlan 100 smart
     ```
   - Add the upstream port to the VLAN.
     ```
     huawei(config)#port vlan 100 0/19 0-2
     ```
   - Configure the native VLAN.

Copyright © Huawei Technologies Co., Ltd.

```
huawei(config)#interface giu 0/19
huawei(config-if-giu-0/19)#native-vlan 0 vlan 100
huawei(config-if-giu-0/19)#native-vlan 1 vlan 100
huawei(config-if-giu-0/19)#native-vlan 2 vlan 100huawei(config-if-giu-0/19)
#quit
```

- Create the traffic profile.

```
huawei(config)#traffic table ip index 8 cir off priority 5 priority-policy
local-Setting
```

- Add ADSL2+ port 2 and 3 to VLAN 100.

```
huawei(config)#service-port 100 vlan 100 adsl 0/2/2 vpi 0 vci 35 rx-cttr 8
tx-cttr 8
huawei(config)#service-port 101 vlan 100 adsl 0/2/3 vpi 0 vci 35 rx-cttr 8
tx-cttr 8
```

3. Configure the multicast service.

- Enable the multicast proxy.

```
huawei(config)#multicast-vlan 100
huawei(config-mvlan100)#igmp mode proxy
  Are you sure to change IGMP mode?(y/n)[n]:y
```

- Add the upstream port.

```
huawei(config-mvlan100)#igmp default uplink-port 0/20/0
huawei(config-mvlan100)#igmp uplink-port 0/20/0
huawei(config-mvlan100)#quit
huawei(config)#btv
huawei(config-btv)#igmp uplink-port-mode mstp
Are you sure to change the uplink port mode?(y/n)[n]:y
```

- Configure the preview parameters.

  In this example, set the preview authority profile 1 with the preview duration for the program to 150s, the number of preview attempts to 6 each day, and the preview interval to 60s.

```
huawei(config-btv)#igmp preview-profile add index 1 duration 150 times 6
interval 60
huawei(config-btv)#igmp preview auto-reset-time 00:00:00
```

- Configure the program library.

```
huawei(config-btv)#quit
huawei(config)#multicast-vlan 100
huawei(config-mvlan100)#igmp program add name program1 ip 224.1.1.1
sourceip 10.10.10.10
huawei(config-mvlan100)#igmp program add name program2 ip 224.1.1.2
sourceip 10.10.10.10
huawei(config-mvlan100)#igmp program add name program3 ip 224.1.1.3
sourceip 10.10.10.10 preview-profile 1
```

- Configure the authority profile.

```
huawei(config-mvlan100)#quit
huawei(config)#btv
huawei(config-btv)#igmp profile profile-name profile0 program-name program1
watch
huawei(config-btv)#igmp profile profile-name profile0 program-name program2
watch
huawei(config-btv)#igmp profile profile-name profile0 program-name program3
preview
```

- Configure the multicast user.

```
huawei(config-btv)#igmp policy service-port 100 normal
huawei(config-btv)#igmp policy service-port 101 normal
huawei(config-btv)#igmp user add port 0/2/3 adsl 0 35 no-auth
huawei(config-btv)#igmp user add port 0/2/2 adsl 0 35 auth
huawei(config-btv)#igmp user bind-profile port 0/2/2 profile-name profile0
huawei(config-btv)#quit
huawei(config)#multicast-vlan 100
```


Copyright © Huawei Technologies Co., Ltd.

```
huawei(config-mvlan100)#igmp multicast-vlan member port 0/2/2
huawei(config-mvlan100)#igmp multicast-vlan member port 0/2/3
```

Step 14 Configure the subtending multicast service.

In the MSTP ring network, MA5600T/MA5603T/MA5608T-1 is subtended with MA5600T/MA5603T/MA5608T-3, and MA5600T/MA5603T/MA5608T-3 is subtended with MA5600T/MA5603T/MA5608T-4. According to the data plan, MA5600T/MA5603T/MA5608T-4 provides the multicast service. In this way, it is necessary to configure the multicast subtending on MA5600T/MA5603T/MA5608T-1 first.

1. Add the upstream port.

   The upstream port is already added in **Step 13.3**. It is unnecessary to configure it again.

2. Configure the IGMP proxy.

   The IGMP proxy is already configured in **Step 13.3**. It is unnecessary to configure it again.

3. Configure the program library.

   The program library is already configured in **Step 13.3**. It is unnecessary to configure it again.

4. Configure the multicast for the subtending port.

   - Specify a subtending port.

     ```
     huawei(config-mvlan100)#quit
     huawei(config)#btv
     huawei(config-btv)#igmp cascade-port 0/19/0
     huawei(config-btv)#igmp cascade-port 0/19/1
     ```

   - Modify the subtending port.

     ```
     huawei(config-btv)#igmp cascade-port modify 0/19/0 static enable
     huawei(config-btv)#igmp cascade-port modify 0/19/1 static enable
     ```

Step 15 Save the data.

```
huawei(config-btv)#quit
huawei(config)#save
```

----End

5.4 Configuring MA5600T/MA5603T/MA5608T-2

This topic describes how to configure MA5600T/MA5603T/MA5608T-2.

Procedure

Step 1 Confirm the board.

```
huawei>enable
huawei#config
huawei(config)#board confirm 0
```

Step 2 Configure the NMS.

1. Configure the IP address of the inband NMS interface.

   - Create the NMS VLAN.

     ```
     huawei(config)#vlan 10 standard
     ```

   - Add the upstream port.

     ```
     huawei(config)#port vlan 10 0/19 0-1
     ```

   - Enter NMS VLAN interface mode.

Copyright © Huawei Technologies Co., Ltd.

```
huawei(config)#interface vlanif 10
```

- Configure the IP address of the NMS VLAN interface.

```
huawei(config-if-vlanif10)#ip address 10.10.1.3 255.255.255.0
huawei(config-if-vlanif10)#quit
```

2. Add the route.
   - Configure the route destined to the NMS (Trap destination host).

```
huawei(config)#ip route-static 2.2.2.0 255.255.255.0 10.10.1.1
preference 1
```

   - Configure the route destined to the time server.

```
huawei(config)#ip route-static 4.4.4.0 255.255.255.0 10.10.1.1
preference 1
```

   - Configure the route destined to the log host.

```
huawei(config)#ip route-static 3.3.3.0 255.255.255.0 10.10.1.1
preference 1
huawei(config)#ip route-static 3.3.4.0 255.255.255.0 10.10.1.1
preference 1
```

3. Add the ACL rule.

```
huawei(config)#acl 3050
huawei(config-acl-adv-3050)#rule permit ip source any destination any
huawei(config-acl-adv-3050)#rule deny ip source any destination 10.10.1.2
0.0.0.0
huawei(config-acl-adv-3050)#rule permit ip source 2.2.2.2 0.0.0.0
destination 10.10.1.2 0.0.0.0
huawei(config-acl-adv-3050)#rule permit ip source 2.2.2.3 0.0.0.0
destination 10.10.1.2 0.0.0.0
huawei(config-acl-adv-3050)#rule permit ip source 4.4.4.4 0.0.0.0
destination 10.10.1.2 0.0.0.0
huawei(config-acl-adv-3050)#rule permit ip source 4.4.4.5 0.0.0.0
destination 10.10.1.2 0.0.0.0
huawei(config-acl-adv-3050)#rule permit ip source 3.3.3.3 0.0.0.0
destination 10.10.1.2 0.0.0.0
huawei(config-acl-adv-3050)#rule permit ip source 3.3.4.3 0.0.0.0
destination 10.10.1.2 0.0.0.0
huawei(config-acl-adv-3050)#quit
huawei(config)#packet-filter inbound ip-group 3050 port 0/19/0
huawei(config)#packet-filter inbound ip-group 3050 port 0/19/1
```

4. Configure SNMP.
   - Configure the community name and access authority.

```
huawei(config)#snmp-agent community read public
huawei(config)#snmp-agent community write private
```

   - Configure the contact information.

```
huawei(config)#snmp-agent sys-info contact HW-075512345678
```

   - Configure the device local information.

```
huawei(config)#snmp-agent sys-info location Shenzhen China
```

   - Configure the SNMP version.

     NOTE

     The SNMP version must be the same as that of NMS. In this example, the NMS version is set as SNMP V2C.

```
huawei(config)#snmp-agent sys-info version v2c
```

5. Enable trap sending.

```
huawei(config)#snmp-agent trap enable standard
```

6. Set the trap destination address.

```
huawei(config)#snmp-agent target-host trap-hostname huawei address 2.2.2.2
trap-paramsname abc
```


Copyright © Huawei Technologies Co., Ltd.

```
huawei(config)#snmp-agent target-host trap-hostname huawei123 address 2.2.2.3
trap-paramsname 123
```

7. Set the trap source address.

```
huawei(config)#snmp-agent trap source vlanif 10
```

Step 3 Configure the time server.

```
huawei(config)#ntp-service unicast-server 4.4.4.4 source-interface vlanif 10
huawei(config)#ntp-service unicast-server 4.4.4.5 source-interface vlanif 10
```

Step 4 Configure the log host.

```
huawei(config)#loghost add 3.3.3.3 syslog-1
huawei(config)#loghost activate ip 3.3.3.3
huawei(config)#loghost add 3.3.4.3 syslog-2
huawei(config)#loghost activate ip 3.3.4.3
```

Step 5 Configure the EMU.

This topic uses the fan and the PS4875L power supply as an example to describe how to configure the EMU.

By default, the default slave node number of the fan EMU is 0. In this example, assume that the slave node number is 1. In this case, you need to set the DIP switch of the node address on the fan monitoring unit to 1.

```
huawei(config)#emu add 0 power48751 0 0
huawei(config)#emu add 1 fan 0 1
huawei(config)#interface emu 0
huawei(config-if-power48751-0)#power module-num 2 1 2
huawei(config-if-power48751-0)#quit
```

Step 6 Configure GIU subtending.

MA5600T/MA5603T/MA5608T-1 is subtended with MA5600T/MA5603T/MA5608T-2, MA5600T/MA5603T/MA5608T-3 and MA5600T/MA5603T/MA5608T-4. Therefore, the subtending should be configured.

Step 7 Configure MSTP.

1. Enable the MSTP function.

```
huawei(config)#stp enable
  Change global stp state may active region configuration,it may take
several
minutes,are you sure to change global stp state? [Y/N][N]
Y
```

2. Set the MST region name.

```
huawei(config)#stp region-configuration
huawei(stp-region-configuration)#region-name hwrg
```

3. Configure MSTP instance 1.

```
huawei(stp-region-configuration)#instance 1 vlan 1 to 4094
```

4. Activate the configuration of the MST region.

```
huawei(stp-region-configuration)#active region-configuration
  STP actives region configuration, it may take several minutes,are you sure
to
active region configuration? [Y/N][N]y
huawei(stp-region-configuration)#quit
```

Step 8 Enable PITP.

```
huawei(config)#pitp enable pmode
```

Step 9 Configure ADSL2+ service.

The MA5600T/MA5603T/MA5608T supports the ADSL2+ service of multiple encapsulation modes, such as IPoA, PPPoA, IPoE, and PPPoE. This topic uses the PPPoE mode as an example

Copyright © Huawei Technologies Co., Ltd.

to describe how to configure the ADSL2+ service. For other encapsulation modes, see "**3.1 Example: Configuring the xDSL Internet Access Service**."

1. Configure the ADSL2+ line profile.

   You can configure the ADSL2+ line profile based on your requirements.

```
huawei(config)#adsl line-profile add 10
  Start adding
profile
  Press 'Q' to quit the current configuration and new configuration will
be
neglected
>  Do you want to name the profile (y/n)
[n]:
>    Transmission
mode:
>      0:
Custom
>      1: All (G.
992.1~5,T1.413,ETSI)
>      2: Full rate(G.
992.1/3/5,T1.413,ETSI)
>      3: G.DMT (G.
992.1/3/5)
>      4: G.HS (G.
992.1~5)
>      5: ADSL (G.
992.1~2,ETSI,T1.413)
>      6: ADSL2 & ADSL2+ (G.
992.3~5)
>    Please select (0~6)
[1]:
>  Trellis mode 1-disable 2-enable (1~2)
[2]:
>  Bit swap downstream 1-disable 2-enable (1~2)
[2]:
>  Bit swap upstream 1-disable 2-enable (1~2)
[2]:
>  Please select the form of transmit rate adaptation
downstream:
>  1-fixed, 2-adaptAtStartup, 3-adaptAtRuntime (1~3)
[2]:
>  Please select the form of transmit rate adaptation
upstream:
>  1-fixed, 2-adaptAtStartup, 3-adaptAtRuntime (1~3)
[2]:
>  Will you set SNR margin parameters? (y/n)
[n]:
>  Will you set DPBO parameters? (y/n)
[n]:
>  Will you set power management parameters? (y/n)
[n]:
>  Will you set tone blackout configuration parameter? (y/n)
[n]:
>  Will you set INM downstream parameter? (y/n)
[n]:
>  Will you set RFI notch configuration parameter? (y/n)
[n]:
>  Will you set mode-specific parameters? (y/n)
[n]:
>  Will you set network timing reference? (y/n) [n]:
  Add profile 10 successfully
```

2. Configure the ADSL2+ channel profile.

   You can configure the ADSL2+ channel profile based on your requirements.

Copyright © Huawei Technologies Co., Ltd.

```
huawei(config)#adsl channel-profile add 10
  Start adding
profile
  Press 'Q' to quit the current configuration and new configuration will
be
neglected
>  Do you want to name the profile (y/n)
[n]:n
>  Data path mode 1-ATM, 2-PTM, 3-Both (1~3) [3]:
1
>  Will you set the minimum impulse noise protection? (y/n)
[n]:y
>    Minimum impulse noise protection
downstream:
>    1-noProtection    2-halfSymbol      3-singleSymbol     4-
twoSymbols
>    5-threeSymbols    6-fourSymbols     7-fiveSymbols      8-
sixSymbols
>    9-sevenSymbols    10-eightSymbols   11-nineSymbols     12-
tenSymbols
>    13-elevenSymbols  14-twelveSymbols  15-thirteenSymbols 16-
fourteenSymbols
>    17-fifteenSymbols 18-
sixteenSymbols
>    Please select (1~18) [2]:
4
>    Minimum impulse noise protection
upstream:
>    1-noProtection    2-halfSymbol      3-singleSymbol     4-
twoSymbols
>    5-threeSymbols    6-fourSymbols     7-fiveSymbols      8-
sixSymbols
>    9-sevenSymbols    10-eightSymbols   11-nineSymbols     12-
tenSymbols
>    13-elevenSymbols  14-twelveSymbols  15-thirteenSymbols 16-
fourteenSymbols
>    17-fifteenSymbols 18-
sixteenSymbols
>    Please select (1~18) [2]:
4
>  Will you set interleaving delay parameters? (y/n)
[n]:y
>    Maximum interleaving delay downstream (0~63 ms) [16]:
24
>    Maximum interleaving delay upstream (0~63 ms) [6]:
12
>  Will you set parameters for rate? (y/n)
[n]:y
>    Minimum transmit rate downstream (32~32000 Kbps)
[32]:
>    Minimum reserved transmit rate downstream (32~32000 Kbps)
[32]:
>    Maximum transmit rate downstream (32~32000 Kbps) [24544]:
8000
>    Minimum transmit rate upstream (32~6000 Kbps)
[32]:
>    Minimum reserved transmit rate upstream (32~6000 Kbps)
[32]:
>    Maximum transmit rate upstream (32~6000 Kbps)
[1024]:
>  Will you set rate thresholds? (y/n)
[n]:
>  Will you set retransmission function (y/n)
[n]:
>  Will you set erasure decoding? (y/n) [n]:
  Add profile 10 successfully
```


Copyright © Huawei Technologies Co., Ltd.

3. Configure the ADSL2+ line template.

   Bind the preceding configured line profile and the channel profile together in the line template with the index of 10.

```
huawei(config)#adsl line-template add 10
  Start adding template
  Press 'Q' to quit the current configuration and new configuration will be
neglected
>  Do you want to name the template (y/n) [n]:
>  Please set the line-profile index (1~128) [1]:10
>  Will you set channel configuration parameters? (y/n) [n]:y
>    Please set the channel number (1~2) [1]:1
>    Channel1 configuration parameters:
>    Please set the channel-profile index (1~128) [1]:10
Add template 10 successfully
```

4. Configure the ADSL2+ alarm profile.

   You can configure the ADSL2+ alarm profile based on your requirements. For detailed configuration, see "Configuring an ADSL2+ Alarm Template." This example uses the default alarm profile 1 in the system.

5. Configure the ADSL2+ traffic profile.

   You can configure the ADSL2+ traffic profile by running the **traffic table ip** command based on your requirements.

   In this example, the default profile (profile 6) is used.

6. Activate the ADSL2+ port.

```
huawei(config)#interface adsl 0/2
huawei(config-if-adsl-0/2)#deactivate all
huawei(config-if-adsl-0/2)#alarm-config all 1
huawei(config-if-adsl-0/2)#activate all template-index 10
huawei(config-if-adsl-0/2)#quit
```

7. Configure the upstream port.

   - Configure the GIU board.

     The configuration of the upstream port of the GIU board should be the same as the configuration of the peer device.

     Run the **auto-neg** command to set the port to work in the auto-negotiation mode. If the port does not work in the auto-negotiation mode, change to the GIU config mode and run the **speed** command to change the port rate, and run the **duplex** command to change the port duplex mode.

   - Configure the VLAN.

     The ADSL2+ users of MA5600T/MA5603T/MA5608T-2 use the PPPoE authentication. In this case, the smart VLAN is used to identify the users.

```
huawei(config)#vlan 2020 smart
huawei(config)#port vlan 2020 0/19 0-1
```

8. Add the service port.

   All ports in slot 0/3 provide the ADSL2+ services. To add service ports in batches, run the **multi-service-port** command.

```
huawei(config)#multi-service-port vlan 2020 port 0/2 0-31 vpi 0 vci 35
 rx-cttr 6 tx-cttr 6
```

Step 10 Configure the SHDSL service.

The MA5600T/MA5603T/MA5608T supports the SHDSL service of multiple encapsulation modes, such as IPoA, PPPoA, IPoE, and PPPoE. This topic uses the PPPoE mode as an example

Copyright © Huawei Technologies Co., Ltd.

to describe how to configure the SHDSL service. For other encapsulation modes, see "**3.1 Example: Configuring the xDSL Internet Access Service**."

1. Configure the SHDSL line profile.

   To configure the SHDSL line profile, run the **shdsl line-profile add** or **shdsl line-profile quickadd** command.

```
huawei(config)#shdsl line-profile quickadd 10 line two-wire rate 2048 2048
psd
symmetric transmission Annex-A remote disable probe disable snr-margin ds-curr
10 ds-worst
 10 us-curr 10 us-worst 10 bitmap 0x03
```

2. Configure the SHDSL alarm profile.

   To configure the SHDSL alarm profile, run the **shdsl alarm-profile add** command.

   In this example, the default profile (profile 1) is used.

3. Configure the SHDSL traffic profile.

   To configure the SHDSL traffic profile, run the **traffic table ip** command.

   In this example, the default profile (profile 1) is used.

4. Activate the SHDSL port.

```
huawei(config)#interface shl 0/5
huawei(config-if-shl-0/5)#deactivate all
huawei(config-if-shl-0/5)#alarm-config all 1
huawei(config-if-shl-0/5)#activate all 10
huawei(config-if-shl-0/5)#quit
```

5. Configure the upstream port.

   The SHDSL users of MA5600T/MA5603T/MA5608T-2 use the PPPoE authentication. In this case, the smart VLAN is used to identify the users.

```
huawei(config)#vlan 3020 smart
huawei(config)#port vlan 3020 0/19 0-1
```

6. Add the service port.

   - Ports 0-15 of the SHDSL board in 0/5 provide the SHDSL services.
   - To add service ports in batches, run the **multi-service-port** command.

```
huawei(config)#multi-service-port vlan 3020 port 0/5 0-15 vpi 0 vci 35
rx-cttr 6 tx-cttr 6
```

Step 11 Configure the POTS service.

1. Configure the upstream ports of the media stream and the signaling flow.

```
huawei(config)#vlan 1600 smart
huawei(config)#port vlan 1600 0/19 0
huawei(config)#interface vlanif 1600
huawei(config-if-vlanif1600)#ip address 10.176.6.33 24
huawei(config-if-vlanif1600)#quit
```

2. Configure the static route destined to the MGC.

   NOTE

   When the MGC and the MG are in the same network segment, you do not need to configure the static route.

```
huawei(config)#ip route-static 10.30.80.0 255.255.255.0 10.176.6.62
```

3. Configure the media IP address pool and the signaling IP address pool.

```
huawei(config)#voip
huawei(config-voip)#ip address media 10.176.6.33 10.176.6.62
```


Copyright © Huawei Technologies Co., Ltd.

```
huawei(config-voip)#ip address signaling 10.176.6.33
huawei(config-voip)#quit
```

4. Configure the MG interface.

   Add an MG interface.

   ```
   huawei(config)#interface h248 0
     Are you sure to add MG interface? (y/n)[n]:y
   ```

   Configure the MG interface attributes.

   ```
   huawei(config-if-h248-0)#if-h248 attribute mgip 10.176.6.33 mgport 2944 code
   text
   transfer udp primary-mgc-ip1 10.30.80.65 primary-mgc-port 2944 mg-media-ip1
   10.176.6.33
   ```

   Configure the software parameters of the MG interface (in this example, only parameter 20 is configured, and other parameters use the default values).

   ```
   huawei(config-if-h248-0)#mg-software parameter 20 2
   ```

5. Reset the MG interface.

   NOTE

   After configuring the MG interface, you need to reset the interface to validate the configuration.

   ```
   huawei(config-if-h248-0)#reset coldstart
     Are you sure to reset MG interface?(y/n)[n]:y
   huawei(config-if-h248-0)#quit
   ```

6. Configure the data of PSTN user.

   ```
   huawei(config)#esl user
   huawei(config-esl-user)#mgpstnuser batadd 0/3/0 0/3/31 0 terminalid 0 telno
   88660032
   huawei(config-esl-user)#quit
   ```

Step 12 Configure the stacking multi-ISPs wholesale service.

ISP1 provides users of ports 0/2/0 to 0/2/10 on board with the multi-ISP wholesale service. ISP2 provides users of ports 11-20 to with the multi-ISP wholesale service. ISP3 provides users of port 21-30 with the multi-ISP wholesale service.

1. Create a VLAN and set the attribute as stacking.

   ```
   huawei(config)#vlan 60 to 62 smart
   huawei(config)#vlan attrib 60 to 62 stacking
   ```

2. Add the upstream port.

   ```
   huawei(config)#port vlan 60 to 62 0/19 0-1
   ```

3. Add the service port.

   ```
   huawei(config)#multi-service-port vlan 60 port 0/2 0-10 vpi 0 vci 35 rx-cttr 6
   tx-cttr 6
   huawei(config)#multi-service-port vlan 61 port 0/2 11-20 vpi 0 vci 35 rx-cttr
   6 tx-cttr 6
   huawei(config)#multi-service-port vlan 62 port 0/2 21-30 vpi 0 vci 35 rx-cttr
   6 tx-cttr 6
   ```

4. Configure the inner label.

   ```
   huawei(config)#stacking label vlan 60 baselabel 111
   huawei(config)#stacking label vlan 61 baselabel 112
   huawei(config)#stacking label vlan 62 baselabel 113
   ```

Step 13 Configure the triple play service.

After the configuration, the following results should be achieved: Users of ports 0/2/16 can watch the programs stored on servers 224.1.1.1 and 224.1.1.2, and can preview the programs stored on server 224.1.1.3.

Copyright © Huawei Technologies Co., Ltd.

1. Configure the upstream port and the VLAN.

```
huawei(config)#vlan 100 smart
huawei(config)#port vlan 100 0/19 0-1
huawei(config)#vlan 101 mux
huawei(config)#port vlan 101 0/19 0-1
huawei(config)#vlan 102 smart
huawei(config)#port vlan 102 0/19 0-1
```

2. Configure the traffic table.

   The voice service has the highest priority, and the Internet access service has the lowest priority.

   Assume that the Internet access service uses traffic table 6, with the priority of 0. The following shows how to create the traffic tables for the voice service and the video service respectively.

```
huawei(config)#traffic table ip index 7 cir 1024 priority 7
priority-policy local-Setting
huawei(config)#traffic table ip index 8 cir off priority 5 priority-policy
local-Setting
```

3. Configure the service port.

```
huawei(config)#service-port vlan 100 adsl 0/2/31 vpi 0 vci 35 rx-cttr 8 tx-cttr
8
huawei(config)#service-port vlan 101 adsl 0/2/31 vpi 0 vci 36 rx-cttr 6 tx-cttr
6
huawei(config)#service-port vlan 102 adsl 0/2/31 vpi 0 vci 37 rx-cttr 7 tx-cttr
7
```

4. Configure the DHCP relay mode for the video service.

   - Enable the DHCP mode.

```
huawei(config)#dhcp mode layer-3 option60
```

   - Configure the DHCP server.

```
huawei(config)#dhcp-server 1 ip 10.1.1.2 10.1.1.3
huawei(config)#dhcp domain video
huawei(config-dhcp-domain-video)#dhcp-server 1
huawei(config-dhcp-domain-video)#quit
```

   - Configure the gateway mapped to the DHCP domain.

```
huawei(config)#interface vlanif 100
huawei(config-if-vlanif100)#ip address 10.1.1.1 24
huawei(config-if-vlanif100)#dhcp domain video gateway 10.1.1.1
huawei(config-if-vlanif100)#quit
```

   - Enable the DHCP option82 function.

```
huawei(config)#dhcp option82 enable
huawei(config)#raio-mode xdsl-port-rate
```

5. Configure the DHCP relay mode for the voice service.

   - Configure the DHCP server.

```
huawei(config)#dhcp-server 2 ip 10.4.4.2 10.4.4.3
huawei(config)#dhcp domain voice
huawei(config-dhcp-domain-voice)#dhcp-server 2
huawei(config-dhcp-domain-voice)#quit
```

   - Configure the gateway mapped to the DHCP domain.

```
huawei(config)#interface vlanif 102
huawei(config-if-vlanif102)#ip address 10.4.4.1 24
huawei(config-if-vlanif102)#dhcp domain voice gateway 10.4.4.1
huawei(config-if-vlanif102)#quit
```

6. Configure the multicast service.

   - Enable the multicast proxy.

```
huawei(config)#multicast-vlan 100
huawei(config-mvlan100)#igmp mode proxy
```


Copyright © Huawei Technologies Co., Ltd.

```
  Are you sure to change IGMP mode?(y/n)[n]:y
huawei(config-mvlan100)#quit
```

- Configure the preview parameters.

  In this example, configure preview authority profile 1 with the preview duration for the program to 150s, the number of preview attempts to 6 each day, and the preview interval to 60s.

```
huawei(config)#btv
huawei(config-btv)#igmp preview-profile index 1 duration 150 times 6
interval 60
huawei(config-btv)#igmp preview auto-reset-time 00:00:00
huawei(config-btv)#quit
```

- Configure the program library.

```
huawei(config)#multicast-vlan 100
huawei(config-mvlan100)#igmp program add name program1 ip 224.1.1.1
sourceip 10.10.10.10
huawei(config-mvlan100)#igmp program add name program2 ip 224.1.1.2
sourceip 10.10.10.10
huawei(config-mvlan100)#igmp program add name program3 ip 224.1.1.3
sourceip 10.10.10.10
preview-profile 1
huawei(config-mvlan100)#quit
```

- Configure the authority profile.

```
huawei(config)#btv
huawei(config-btv)#igmp profile profile-name profile0 program-name program1
watch
huawei(config-btv)#igmp profile profile-name profile0 program-name program2
watch
huawei(config-btv)#igmp profile profile-name profile0 program-name program3
preview
```

- Configure the multicast user.

```
huawei(config-btv)#igmp user add port 0/2/15 adsl 0 35 no-auth
huawei(config-btv)#igmp user add port 0/2/16 adsl 0 35 auth
huawei(config-btv)#igmp user bind-profile port 0/2/16 profile-name profile0
huawei(config-btv)#quit
huawei(config)#multicast-vlan 100
huawei(config-mvlan100)#igmp multicast-vlan member port 0/2/15
huawei(config-mvlan100)#igmp multicast-vlan member port 0/2/16
```

Step 14 Configure the subtending multicast service.

In the MSTP ring network, MA5600T/MA5603T/MA5608T-1 is subtended with MA5600T/MA5603T/MA5608T-3, and MA5600T/MA5603T/MA5608T-3 is subtended with MA5600T/MA5603T/MA5608T-4. According to the data plan, MA5600T/MA5603T/MA5608T-4 provides the multicast service. In this way, it is necessary to configure the multicast subtending on MA5600T/MA5603T/MA5608T-2 first.

1. Configure the upstream port.

   The upstream port is already added in **Step 13.6**. It is unnecessary to configure it again.

2. Configure the IGMP proxy.

   The IGMP proxy is already configured in **Step 13.6**. It is unnecessary to configure it again.

3. Configure the program library.

   The program library is already configured in **Step 13.6**. It is unnecessary to configure it again.

4. Configure the multicast for the subtending port.

   - Specify the subtending port.

Copyright © Huawei Technologies Co., Ltd.

```
huawei(config-btv)#igmp cascade-port 0/19/0
huawei(config-btv)#igmp cascade-port 0/19/1
```

- Modify the subtending port.

```
huawei(config-btv)#igmp cascade-port modify 0/19/0 static enable
huawei(config-btv)#igmp cascade-port modify 0/19/1 static enable
huawei(config-btv)#quit
```

Step 15 Save the data.

```
huawei(config)#save
```

----End

5.5 Configuring MA5600T/MA5603T/MA5608T-3

This topic describes how to configure MA5600T/MA5603T/MA5608T-3.

Procedure

Step 1 Confirm the board.

```
huawei>enable
huawei#config
huawei(config)#board confirm 0
```

Step 2 Configure the NMS.

1. Configure the IP address of the inband NMS interface.
   - Create the NMS VLAN.
     ```
     huawei(config)#vlan 10 standard
     ```
   - Add the upstream port.
     ```
     huawei(config)#port vlan 10 0/19 0-1
     ```
   - Enter the NMS VLAN interface mode.
     ```
     huawei(config)#interface vlanif 10
     ```
   - Configure the IP address of the NMS VLAN interface.
     ```
     huawei(config-if-vlanif10)#ip address 10.10.1.4 255.255.255.0
     huawei(config-if-vlanif10)#quit
     ```
2. Add the route.
   - Configure the route destined to the NMS (Trap destination host).
     ```
     huawei(config)#ip route-static 2.2.2.0 255.255.255.0 10.10.1.1
     preference 1
     ```
   - Configure the route destined to the time server.
     ```
     huawei(config)#ip route-static 4.4.4.0 255.255.255.0 10.10.1.1
     preference 1
     ```
   - Configure the route destined to the log host.
     ```
     huawei(config)#ip route-static 3.3.3.0 255.255.255.0 10.10.1.1
     preference 1
     huawei(config)#ip route-static 3.3.4.0 255.255.255.0 10.10.1.1
     preference 1
     ```
3. Add the ACL rule.

```
huawei(config)#acl 3050
huawei(config-acl-adv-3050)#rule permit ip source any destination any
huawei(config-acl-adv-3050)#rule deny ip source any destination 10.10.1.2
0.0.0.0
huawei(config-acl-adv-3050)#rule permit ip source 2.2.2.2 0.0.0.0
destination 10.10.1.2 0.0.0.0
huawei(config-acl-adv-3050)#rule permit ip source 2.2.2.3 0.0.0.0
destination 10.10.1.2 0.0.0.0
```


Copyright © Huawei Technologies Co., Ltd.

```
huawei(config-acl-adv-3050)#rule permit ip source 4.4.4.4 0.0.0.0
destination 10.10.1.2 0.0.0.0
huawei(config-acl-adv-3050)#rule permit ip source 4.4.4.5 0.0.0.0
destination 10.10.1.2 0.0.0.0
huawei(config-acl-adv-3050)#rule permit ip source 3.3.3.3 0.0.0.0
destination 10.10.1.2 0.0.0.0
huawei(config-acl-adv-3050)#rule permit ip source 3.3.4.3 0.0.0.0
destination 10.10.1.2 0.0.0.0
huawei(config-acl-adv-3050)#quit
huawei(config)#packet-filter inbound ip-group 3050 port 0/19/0
huawei(config)#packet-filter inbound ip-group 3050 port 0/19/1
```

4. Configure SNMP.
   - Configure the community name and access authority.
     ```
     huawei(config)#snmp-agent community read public
     huawei(config)#snmp-agent community write private
     ```
   - Configure the contact information.
     ```
     huawei(config)#snmp-agent sys-info contact HW-075512345678
     ```
   - Configure the device local information.
     ```
     huawei(config)#snmp-agent sys-info location Shenzhen China
     ```
   - Configure the SNMP version.

     The SNMP version must be the same as the SNMP version of the NMS. In this example, the NMS version is set as SNMP V2C.

     ```
     huawei(config)#snmp-agent sys-info version v2c
     ```
5. Enable trap sending.
   ```
   huawei(config)#snmp-agent trap enable standard
   ```
6. Set the trap destination address.
   ```
   huawei(config)#snmp-agent target-host trap-hostname huawei address 2.2.2.2
   trap-paramsname abc
   huawei(config)#snmp-agent target-host trap-hostname huawei123 address 2.2.2.3
   trap-paramsname 123
   ```
7. Set the trap source address.
   ```
   huawei(config)#snmp-agent trap source vlanif 10
   ```

Step 3 Configure the time server.

```
huawei(config)#ntp-service unicast-server 4.4.4.4 source-interface
vlanif 10
huawei(config)#ntp-service unicast-server 4.4.4.5 source-interface
vlanif 10
```

Step 4 Configure the log host.

```
huawei(config)#loghost add 3.3.3.3 syslog-1
huawei(config)#loghost activate ip 3.3.3.3
huawei(config)#loghost add 3.3.4.3 syslog-2
huawei(config)#loghost activate ip 3.3.4.3
```

Step 5 Configure the EMU.

This topic uses the fan and the PS4875L power supply as examples to describe how to configure the environment monitoring unit (EMU).

By default, the default slave node number of the fan EMU is 0. In this example, assume that the slave node number is 1. In this case, you need to set the DIP switch of the node address on the fan monitoring unit as 1.

```
huawei(config)#emu add 0 power4875l 0 0
huawei(config)#emu add 1 fan 0 1
huawei(config)#interface emu 0
```


Copyright © Huawei Technologies Co., Ltd.

```
huawei(config-if-power4875l-0)#power module-num 2 1 2
huawei(config-if-power4875l-0)#quit
```

Step 6 Configure GIU subtending.

MA5600T/MA5603T/MA5608T-1 is subtended with MA5600T/MA5603T/MA5608T-2, MA5600T/MA5603T/MA5608T-3 and MA5600T/MA5603T/MA5608T-4. Therefore, the subtending should be configured.

```
huawei(config)#vlan 60 to 62 standard
huawei(config)#port vlan 60 to 62 0/19 0-1
huawei(config)#vlan 101 to 102 standard
huawei(config)#port vlan 101 to 102 0/19 0-1
huawei(config)#vlan 100 standard
huawei(config)#port vlan 100 0/19 0-1
```

Step 7 Enable MSTP.

1. Enable the MSTP function.

```
huawei(config)#stp enable
  Change global stp state may active region configuration,it may take
several
minutes,are you sure to change global stp state? [Y/N][N]
Y
```

2. Set the MST region name.

```
huawei(config)#stp region-configuration
huawei(stp-region-configuration)#region-name hwrg
```

3. Configure MSTP instance 1.

```
huawei(stp-region-configuration)#instance 1 vlan 1 to 4094
```

4. Activate the configuration of the MST region.

```
huawei(stp-region-configuration)#active region-configuration
  STP actives region configuration, it may take several minutes,are you sure
to
active region configuration? [Y/N][N]y
huawei(stp-region-configuration)#quit
```

Step 8 Configure the ADSL2+ service.

The MA5600T/MA5603T/MA5608T supports the ADSL2+ service of multiple encapsulation modes, such as IPoA, PPPoA, IPoE, and PPPoE. This topic uses the PPPoE mode as an example to describe how to configure the ADSL2+ service. For other encapsulation modes, see "**3.1 Example: Configuring the xDSL Internet Access Service**."

1. Configure the ADSL2+ line profile.

   You can configure the ADSL2+ line profile based on your requirements.

```
huawei(config)#adsl line-profile add 10
  Start adding
profile
  Press 'Q' to quit the current configuration and new configuration will
be
neglected
>  Do you want to name the profile (y/n)
[n]:
>    Transmission
mode:
>      0:
Custom
>      1: All (G.
992.1~5,T1.413,ETSI)
>      2: Full rate(G.
992.1/3/5,T1.413,ETSI)
>      3: G.DMT (G.
```


Copyright © Huawei Technologies Co., Ltd.

```
992.1/3/5)
>      4: G.HS (G.
992.1~5)
>      5: ADSL (G.
992.1~2,ETSI,T1.413)
>      6: ADSL2 & ADSL2+ (G.
992.3~5)
>    Please select (0~6)
[1]:
>  Trellis mode 1-disable 2-enable (1~2)
[2]:
>  Bit swap downstream 1-disable 2-enable (1~2)
[2]:
>  Bit swap upstream 1-disable 2-enable (1~2)
[2]:
>  Please select the form of transmit rate adaptation
downstream:
>  1-fixed, 2-adaptAtStartup, 3-adaptAtRuntime (1~3)
[2]:
>  Please select the form of transmit rate adaptation
upstream:
>  1-fixed, 2-adaptAtStartup, 3-adaptAtRuntime (1~3)
[2]:
>  Will you set SNR margin parameters? (y/n)
[n]:
>  Will you set DPBO parameters? (y/n)
[n]:
>  Will you set power management parameters? (y/n)
[n]:
>  Will you set tone blackout configuration parameter? (y/n)
[n]:
>  Will you set INM downstream parameter? (y/n)
[n]:
>  Will you set RFI notch configuration parameter? (y/n)
[n]:
>  Will you set mode-specific parameters? (y/n)
[n]:
>  Will you set network timing reference? (y/n) [n]:
  Add profile 10 successfully
```

2. Configure the ADSL2+ channel profile.

   You can configure the ADSL2+ channel profile based on your requirements.

```
huawei(config)#adsl channel-profile add 10
  Start adding
profile
  Press 'Q' to quit the current configuration and new configuration will
be
neglected
>  Do you want to name the profile (y/n)
[n]:n
>  Data path mode 1-ATM, 2-PTM, 3-Both (1~3) [3]:
1
>  Will you set the minimum impulse noise protection? (y/n)
[n]:y
>    Minimum impulse noise protection
downstream:
>    1-noProtection    2-halfSymbol      3-singleSymbol     4-
twoSymbols
>    5-threeSymbols    6-fourSymbols     7-fiveSymbols      8-
sixSymbols
>    9-sevenSymbols    10-eightSymbols   11-nineSymbols     12-
tenSymbols
>    13-elevenSymbols  14-twelveSymbols  15-thirteenSymbols 16-
fourteenSymbols
>    17-fifteenSymbols 18-
sixteenSymbols
>    Please select (1~18) [2]:
```


Copyright © Huawei Technologies Co., Ltd.

```
4
>    Minimum impulse noise protection
upstream:
>    1-noProtection    2-halfSymbol      3-singleSymbol     4-
twoSymbols
>    5-threeSymbols    6-fourSymbols     7-fiveSymbols      8-
sixSymbols
>    9-sevenSymbols    10-eightSymbols   11-nineSymbols     12-
tenSymbols
>    13-elevenSymbols  14-twelveSymbols  15-thirteenSymbols 16-
fourteenSymbols
>    17-fifteenSymbols 18-
sixteenSymbols
>    Please select (1~18) [2]:
4
>  Will you set interleaving delay parameters? (y/n)
[n]:y
>    Maximum interleaving delay downstream (0~63 ms) [16]:
24
>    Maximum interleaving delay upstream (0~63 ms) [6]:
12
>  Will you set parameters for rate? (y/n)
[n]:y
>    Minimum transmit rate downstream (32~32000 Kbps)
[32]:
>    Minimum reserved transmit rate downstream (32~32000 Kbps)
[32]:
>    Maximum transmit rate downstream (32~32000 Kbps) [24544]:
8000
>    Minimum transmit rate upstream (32~6000 Kbps)
[32]:
>    Minimum reserved transmit rate upstream (32~6000 Kbps)
[32]:
>    Maximum transmit rate upstream (32~6000 Kbps)
[1024]:
>  Will you set rate thresholds? (y/n)
[n]:
>  Will you set retransmission function (y/n)
[n]:
>  Will you set erasure decoding? (y/n) [n]:
  Add profile 10 successfully
```

3. Configure the ADSL2+ line template.

   The configured ADSL2+ line profile and the ADSL2+ channel profile are bound together in the ADSL2+ line template and the index of the ADSL2+ line template is 10.

```
huawei(config)#adsl line-template add 10
  Start adding template
  Press 'Q' to quit the current configuration and new configuration will be
neglected
>  Do you want to name the template (y/n) [n]:
>  Please set the line-profile index (1~128) [1]:10
>  Will you set channel configuration parameters? (y/n) [n]:y
>    Please set the channel number (1~2) [1]:1
>    Channel1 configuration parameters:
>    Please set the channel-profile index (1~128) [1]:10
Add template 10 successfully
```

4. Configure the ADSL2+ alarm profile.

   You can configure the ADSL2+ alarm profile based on your requirements. For details on the configuration, see "Configuring an ADSL2+ Alarm Template." In this example, the default alarm profile (template 1) is used.

5. Configure the ADSL2+ traffic profile.

   You can configure the ADSL2+ traffic profile by running the **traffic table ip** command based on your requirements.

Copyright © Huawei Technologies Co., Ltd.

In this example, the default profile (profile 6) is used.

6. Activate the ADSL2+ port.

```
huawei(config)#interface adsl 0/3
huawei(config-if-adsl-0/3)#deactivate all
huawei(config-if-adsl-0/3)#alarm-config all 1
huawei(config-if-adsl-0/3)#activate all template-index 10
huawei(config-if-adsl-0/3)#quit
```

7. Configure the upstream port.

   - Configure the GIU board.

     The configuration of the upstream port of the GIU board should be the same as that of the peer device.

     Run the **auto-neg** command to set the port to work in the auto-negotiation mode.

     If the port does not work in the auto-negotiation mode, change to the GIU config mode and run the **speed** command to change the port rate, and run the **duplex** command to change the port duplex mode.

   - Configure the VLAN.

     The ADSL2+ users of MA5600T/MA5603T/MA5608T-3 use the VLAN authentication. In this case, the smart VLAN is used to identify the users.

```
huawei(config)#vlan 2030 smart
huawei(config)#port vlan 2030 0/19 0
```

8. Add the service port.

   All ports in slot 0/3 provide the ADSL2+ service. To add service ports in batches, run the **multi-service-port** command.

```
huawei(config)#multi-service-port from-vlan 1000 port 0/3 0-31 vpi 0 vci 35
rx-cttr 6 tx-cttr 6
```

Step 9 Configure the SHDSL service.

The MA5600T/MA5603T/MA5608T supports the SHDSL service of multiple encapsulation modes, such as IPoA, PPPoA, IPoE, and PPPoE. This topic uses the PPPoE mode as an example to describe how to configure the SHDSL service. For other encapsulation modes, see "**3.1 Example: Configuring the xDSL Internet Access Service**."

1. Configure the SHDSL line profile.

   To configure the SHDSL line profile, run the **shdsl line-profile add** or **shdsl line-profile quickadd** command.

```
huawei(config)#shdsl line-profile quickadd 10 line two-wire rate 2048 2048
psd
symmetric transmission Annex-A remote disable probe disable snr-margin ds-curr
10 ds-worst
 10 us-curr 10 us-worst 10 bitmap 0x03
```

2. Configure the SHDSL alarm profile.

   To configure the SHDSL alarm profile, run the **shdsl alarm-profile add** command.

   In this example, the default profile (profile 1) is used.

3. Configure the SHDSL traffic profile.

   To configure the SHDSL traffic profile, run the **traffic table ip** command.

   In this example, the default profile (profile 1) is used.

4. Activate the SHDSL port.

Copyright © Huawei Technologies Co., Ltd.

```
huawei(config)#interface shl 0/5
huawei(config-if-shl-0/5)#deactivate all
huawei(config-if-shl-0/5)#alarm-config all 1
huawei(config-if-shl-0/5)#activate all 10
huawei(config-if-shl-0/5)#quit
```

5. Configure the upstream port.

   The SHDSL users of MA5600T/MA5603T/MA5608T-3 use the VLAN authentication. In this case, the smart VLAN is used to identify the users.

   ```
   huawei(config)#vlan 3030 smart
   huawei(config)#port vlan 3030 0/19 0-1
   ```

6. Add the service port.

   Ports 0-15 in slots 0/5 provide the SHDSL service. To add service ports in batches, run the **multi-service-port** command.

   ```
   huawei(config)#multi-service-port vlan 3030 port 0/5 0-15 vpi 0 vci 35 user-encap
   pppoe rx-cttr 6 tx-cttr 6
   ```

Step 10 Configure the GPON service.

1. Configure the service VLAN and the upstream port.

   ```
   huawei(config)#vlan 1530 smart
   huawei(config)#port vlan 1530 0/19 0
   ```

2. Configure the DBA profile.

   ```
   huawei(config)#dba-profile add profile-id 10 type1 fix 102400
   ```

3. Configure the alarm threshold profile.

   - When you need to configure the alarm threshold value to monitor the performance statistics of the activated ONT line, run the **gpon alarm-profile add** command to configure the GPON alarm threshold profile.
   - In the default GPON alarm threshold profile 1, all alarm thresholds are set to 0, which indicates that no alarm is reported.
   - In this example, the default alarm threshold profile is used. You do not need to configure it.

4. Configure the GPON traffic profile.

   ```
   huawei(config)#traffic table ip index 8 cir 10240 priority 0 priority-policy tag-In-Package
   ```

5. Add an ONT.

   NOTE

   - You can add an ONT in two ways: run the **ont add** command to add an ONT offline or run the **ont confirm** command to confirm an ONT that is in the auto-find state.
   - You need to run the **port ont-auto-find** command in the GPON mode to enable the auto-find function of the ONT.

   ```
   huawei(config)#interface gpon 0/18
   huawei(config-if-gpon-0/18)#ont add 1 sn-auth hwhw-10101010 profile-id 2
   ```

   NOTE

   In this example, the ONT uses the default capability set profile 2. You can run the **ont-profile add** command to configure the capability set profile of the ONT based on your requirements.

6. Bind the alarm threshold profile.

   ```
   huawei(config-if-gpon-0/18)#ont alarm-profile 1 0 profile-id 1
   ```

7. Bind the DBA profile.

Copyright © Huawei Technologies Co., Ltd.

```
huawei(config-if-gpon-0/18)#tcont bind-profile 1 0 1 profile-id 10
```

8. Divide the ONT port VLAN.

```
huawei(config-if-gpon-0/18)#ont port vlan 1 0 eth 10 0
huawei(config-if-gpon-0/18)#ont port native-vlan 1 0 eth 0 vlan 1530
```

9. Configure the GEM port.

```
huawei(config-if-gpon-0/18)#gemport add 1 gemportid 150 eth
```

10. Bind the GEM port to an ONT T-CONT.

NOTE

In the actual application, if the ONT terminal does not support the priority queue scheduling, you can use the CAR to limit the rate when binding the GEM port to the ONT T-CONT.

```
huawei(config-if-gpon-0/18)#ont gemport bind 1 0 150 1 priority-queue 3
```

11. Create the mapping between the GEM port and the service stream.

```
huawei(config-if-gpon-0/18)#ont gemport mapping 1 0 150 vlan 1530
huawei(config-if-gpon-0/18)#quit
```

12. Add the service port.

```
huawei(config)#service-port vlan 1530 gpon 0/18/0 gemport 150 multi-service
user-vlan 10 rx-cttr 5 tx-cttr 8
```

Step 11 Configure the subtending multicast service.

1. Configure the multicast service.
   - Configure the native VLAN.

```
huawei(config)#interface giu 0/19
huawei(config-if-giu-0/19)#native-vlan 0 vlan 100
huawei(config-if-giu-0/19)#native-vlan 1 vlan 100
huawei(config-if-giu-0/19)#quit
```

   - Enable the multicast proxy.

```
huawei(config)#multicast-vlan 100
huawei(config-mvlan100)#igmp mode proxy
  Are you sure to change IGMP mode?(y/n)[n]:y
```

   - Configure the program library.

```
huawei(config-mvlan100)#igmp program add name program1 ip 224.1.1.1
sourceip 10.10.10.10
huawei(config-mvlan100)#igmp program add name program2 ip 224.1.1.2
sourceip 10.10.10.10
huawei(config-mvlan100)#igmp program add name program3 ip 224.1.1.3
sourceip 10.10.10.10
huawei(config-mvlan100)#quit
```

2. Configure the subtending multicast.
   - Specify the subtending ports.

```
huawei(config)#btv
huawei(config-btv)#igmp cascade-port 0/19/0
huawei(config-btv)#igmp cascade-port 0/19/1
huawei(config-btv)#igmp cascade-port 0/20/0
```

   - Modify the subtending ports.

```
huawei(config-btv)#igmp cascade-port modify 0/19/0 static enable
huawei(config-btv)#igmp cascade-port modify 0/19/1 static enable
huawei(config-btv)#igmp cascade-port modify 0/20/0 static enable
huawei(config-btv)#quit
```

Step 12 Save the data.

```
huawei(config)#save
```

----End

Copyright © Huawei Technologies Co., Ltd.

5.6 Configuring MA5600T/MA5603T/MA5608T-4

This topic describes how to configure MA5600T/MA5603T/MA5608T-4.

Procedure

Step 1 Confirm the board.

```
huawei>enable
huawei#config
huawei(config)#board confirm 0
```

Step 2 Configure the NMS.

1. Configure the IP address of the inband NMS interface.
   - Create the NMS VLAN.
     ```
     huawei(config)#vlan 10 standard
     ```
   - Add the upstream port.
     ```
     huawei(config)#port vlan 10 0/19 0
     ```
   - Enter NMS VLAN interface mode.
     ```
     huawei(config)#interface vlanif 10
     ```
   - Configure the IP address of the NMS VLAN interface.
     ```
     huawei(config-if-vlanif10)#ip address 10.10.1.5 255.255.255.0
     huawei(config-if-vlanif10)#quit
     ```
2. Add the route.
   - Configure the route destined to the NMS (Trap destination host).
     ```
     huawei(config)#ip route-static 2.2.2.0 255.255.255.0 10.10.1.1
     preference 1
     ```
   - Configure the route destined to the time server.
     ```
     huawei(config)#ip route-static 4.4.4.0 255.255.255.0 10.10.1.1
     preference 1
     ```
   - Configure the route destined to the log host.
     ```
     huawei(config)#ip route-static 3.3.3.0 255.255.255.0 10.10.1.1
     preference 1
     huawei(config)#ip route-static 3.3.4.0 255.255.255.0 10.10.1.1
     preference 1
     ```
3. Add the ACL rule.

```
huawei(config)#acl 3050
huawei(config-acl-adv-3050)#rule permit ip source any destination any
huawei(config-acl-adv-3050)#rule deny ip source any destination 10.10.1.2
0.0.0.0
huawei(config-acl-adv-3050)#rule permit ip source 2.2.2.2 0.0.0.0
destination 10.10.1.2 0.0.0.0
huawei(config-acl-adv-3050)#rule permit ip source 2.2.2.3 0.0.0.0
destination 10.10.1.2 0.0.0.0
huawei(config-acl-adv-3050)#rule permit ip source 4.4.4.4 0.0.0.0
destination 10.10.1.2 0.0.0.0
huawei(config-acl-adv-3050)#rule permit ip source 4.4.4.5 0.0.0.0
destination 10.10.1.2 0.0.0.0
huawei(config-acl-adv-3050)#rule permit ip source 3.3.3.3 0.0.0.0
destination 10.10.1.2 0.0.0.0
huawei(config-acl-adv-3050)#rule permit ip source 3.3.4.3 0.0.0.0
destination 10.10.1.2 0.0.0.0
huawei(config-acl-adv-3050)#quit
huawei(config)#packet-filter inbound ip-group 3050 port 0/19/0
huawei(config)#packet-filter inbound ip-group 3050 port 0/19/1
```


Copyright © Huawei Technologies Co., Ltd.

4. Configure the SNMP.
   - Configure the community name and access authority.
     ```
     huawei(config)#snmp-agent community read public
     huawei(config)#snmp-agent community write private
     ```
   - Configure the contact information.
     ```
     huawei(config)#snmp-agent sys-info contact HW-075512345678
     ```
   - Configure the device local information.
     ```
     huawei(config)#snmp-agent sys-info location Shenzhen China
     ```
   - Configure the SNMP version.

     The SNMP version must be the same as that of NMS. In this example, the NMS version is set as SNMP V2C.

     ```
     huawei(config)#snmp-agent sys-info version v2c
     ```
5. Enable trap sending.
   ```
   huawei(config)#snmp-agent trap enable standard
   ```
6. Set the trap destination address.
   ```
   huawei(config)#snmp-agent target-host trap-hostname huawei address 2.2.2.2
   trap-paramsname abc
   huawei(config)#snmp-agent target-host trap-hostname huawei123 address 2.2.2.3
   trap-paramsname 123
   ```
7. Set the trap source address.
   ```
   huawei(config)#snmp-agent trap source vlanif 10
   ```

Step 3 Configure the time server.

```
huawei(config)#ntp-service unicast-server 4.4.4.4 source-interface vlanif 10
huawei(config)#ntp-service unicast-server 4.4.4.5 source-interface vlanif 10
```

Step 4 Configure the log host.

```
huawei(config)#loghost add 3.3.3.3 syslog-1
huawei(config)#loghost activate ip 3.3.3.3
huawei(config)#loghost add 3.3.4.3 syslog-2
huawei(config)#loghost activate ip 3.3.4.3
```

Step 5 Configure the EMU.

This topic uses the fan and the PS4875L power supply as examples to describe how to configure the environment monitoring unit (EMU).

By default, the default slave node number of the fan EMU is 0. In this example, assume that the slave node number is 1. In this case, you need to set the DIP switch of the node address on the fan monitoring unit as 1.

```
huawei(config)#emu add 0 power4875l 0 0
huawei(config)#emu add 1 fan 0 1
huawei(config)#interface emu 0
huawei(config-if-power4875l-0)#power module-num 2 1 2
huawei(config-if-power4875l-0)#quit
```

Step 6 Enable PITP.

```
huawei(config)#pitp enable pmode
```

Step 7 Configure the ADSL2+ service.

The MA5600T/MA5603T/MA5608T supports the ADSL2+ service of multiple encapsulation modes, such as IPoA, PPPoA, IPoE, and PPPoE. This topic uses the PPPoE mode as an example to describe how to configure the ADSL2+ service. For other encapsulation modes, see "**3.1 Example: Configuring the xDSL Internet Access Service**."

Copyright © Huawei Technologies Co., Ltd.

1. Configure the ADSL2+ line profile.

   You can configure the ADSL2+ line profile based on your requirements.

```
huawei(config)#adsl line-profile add 10
  Start adding
profile
  Press 'Q' to quit the current configuration and new configuration will
be
neglected
>  Do you want to name the profile (y/n)
[n]:
>    Transmission
mode:
>      0:
Custom
>      1: All (G.
992.1~5,T1.413,ETSI)
>      2: Full rate(G.
992.1/3/5,T1.413,ETSI)
>      3: G.DMT (G.
992.1/3/5)
>      4: G.HS (G.
992.1~5)
>      5: ADSL (G.
992.1~2,ETSI,T1.413)
>      6: ADSL2 & ADSL2+ (G.
992.3~5)
>    Please select (0~6)
[1]:
>  Trellis mode 1-disable 2-enable (1~2)
[2]:
>  Bit swap downstream 1-disable 2-enable (1~2)
[2]:
>  Bit swap upstream 1-disable 2-enable (1~2)
[2]:
>  Please select the form of transmit rate adaptation
downstream:
>  1-fixed, 2-adaptAtStartup, 3-adaptAtRuntime (1~3)
[2]:
>  Please select the form of transmit rate adaptation
upstream:
>  1-fixed, 2-adaptAtStartup, 3-adaptAtRuntime (1~3)
[2]:
>  Will you set SNR margin parameters? (y/n)
[n]:
>  Will you set DPBO parameters? (y/n)
[n]:
>  Will you set power management parameters? (y/n)
[n]:
>  Will you set tone blackout configuration parameter? (y/n)
[n]:
>  Will you set INM downstream parameter? (y/n)
[n]:
>  Will you set RFI notch configuration parameter? (y/n)
[n]:
>  Will you set mode-specific parameters? (y/n)
[n]:
>  Will you set network timing reference? (y/n) [n]:
  Add profile 10 successfully
```

2. Configure the ADSL2+ channel profile.

   You can configure the ADSL2+ channel profile based on your requirements.

```
huawei(config)#adsl channel-profile add 10
  Start adding
profile
  Press 'Q' to quit the current configuration and new configuration will
```


Copyright © Huawei Technologies Co., Ltd.

```
be
neglected
>  Do you want to name the profile (y/n)
[n]:n
>  Data path mode 1-ATM, 2-PTM, 3-Both (1~3) [3]:
1
>  Will you set the minimum impulse noise protection? (y/n)
[n]:y
>    Minimum impulse noise protection
downstream:
>    1-noProtection    2-halfSymbol      3-singleSymbol     4-
twoSymbols
>    5-threeSymbols    6-fourSymbols     7-fiveSymbols      8-
sixSymbols
>    9-sevenSymbols    10-eightSymbols   11-nineSymbols     12-
tenSymbols
>    13-elevenSymbols  14-twelveSymbols  15-thirteenSymbols 16-
fourteenSymbols
>    17-fifteenSymbols 18-
sixteenSymbols
>    Please select (1~18) [2]:
4
>    Minimum impulse noise protection
upstream:
>    1-noProtection    2-halfSymbol      3-singleSymbol     4-
twoSymbols
>    5-threeSymbols    6-fourSymbols     7-fiveSymbols      8-
sixSymbols
>    9-sevenSymbols    10-eightSymbols   11-nineSymbols     12-
tenSymbols
>    13-elevenSymbols  14-twelveSymbols  15-thirteenSymbols 16-
fourteenSymbols
>    17-fifteenSymbols 18-
sixteenSymbols
>    Please select (1~18) [2]:
4
>  Will you set interleaving delay parameters? (y/n)
[n]:y
>    Maximum interleaving delay downstream (0~63 ms) [16]:
24
>    Maximum interleaving delay upstream (0~63 ms) [6]:
12
>  Will you set parameters for rate? (y/n)
[n]:y
>    Minimum transmit rate downstream (32~32000 Kbps)
[32]:
>    Minimum reserved transmit rate downstream (32~32000 Kbps)
[32]:
>    Maximum transmit rate downstream (32~32000 Kbps) [24544]:
8000
>    Minimum transmit rate upstream (32~6000 Kbps)
[32]:
>    Minimum reserved transmit rate upstream (32~6000 Kbps)
[32]:
>    Maximum transmit rate upstream (32~6000 Kbps)
[1024]:
>  Will you set rate thresholds? (y/n)
[n]:
>  Will you set retransmission function (y/n)
[n]:
>  Will you set erasure decoding? (y/n) [n]:
  Add profile 10 successfully
```

3. Configure the ADSL2+ line template.

   The configured ADSL2+ line profile and the ADSL2+ channel profile are bound together in the ADSL2+ line template and the index of the ADSL2+ line template is 10.

Copyright © Huawei Technologies Co., Ltd.

```
huawei(config)#adsl line-template add 10
  Start adding template
  Press 'Q' to quit the current configuration and new configuration will be
neglected
>  Do you want to name the template (y/n) [n]:
>  Please set the line-profile index (1~128) [1]:10
>  Will you set channel configuration parameters? (y/n) [n]:y
>    Please set the channel number (1~2) [1]:1
>    Channel1 configuration parameters:
>    Please set the channel-profile index (1~128) [1]:10
Add template 10 successfully
```

4. Configure the ADSL2+ alarm profile.

   You can configure the ADSL2+ alarm profile based on your requirements. For details on the configuration, see "Configuring an ADSL2+ Alarm Template." In this example, the default alarm profile (template 1) is used.

5. Configure the ADSL2+ traffic profile.

   You can configure the ADSL2+ traffic profile by running the **traffic table ip** command based on your requirements.

   In this example, the default profile (profile 6) is used.

6. Activate the ADSL2+ port.

```
huawei(config)#interface adsl 0/2
huawei(config-if-adsl-0/2)#deactivate all
huawei(config-if-adsl-0/2)#alarm-config all 1
huawei(config-if-adsl-0/2)#activate all template-index 10
huawei(config-if-adsl-0/2)#quit
```

7. Configure the upstream port.

   - Configure the GIU board.

     The configuration of the upstream port of the GIU board should be the same as the configuration of the peer device.
     Run the **auto-neg** command to set the port to work in the auto-negotiation mode.
     If the port does not work in the auto-negotiation mode, change to the GIU config mode and run the **speed** command to change the port rate, and run the **duplex** command to change the port duplex mode.

   - Configure the VLAN.

     The ADSL2+ users of MA5600T/MA5603T/MA5608T-4 adopt the PPPoE authentication. In this case, the smart VLAN is used to identify the users.

```
huawei(config)#vlan 2040 smart
huawei(config)#port vlan 2040 0/19 0
```

8. Add the service port.

   All ports in slot 0/2 provide the ADSL2+ service. To add service ports in batches, run the **multi-service-port** command.

```
huawei(config)#multi-service-port vlan 2040 port 0/2 0-31 vpi 0 vci 35
rx-cttr 6 tx-cttr 6
```

Step 8 Configure the SHDSL service.

The MA5600T/MA5603T/MA5608T supports the SHDSL service of multiple encapsulation modes, such as IPoA, PPPoA, IPoE, and PPPoE. This topic uses the PPPoE mode as an example to describe how to configure the SHDSL service. For other encapsulation modes, see "**3.1 Example: Configuring the xDSL Internet Access Service**."

Copyright © Huawei Technologies Co., Ltd.

1. Configure the SHDSL line profile.

   To configure the SHDSL line profile, run the **shdsl line-profile add** or **shdsl line-profile quickadd** command.

   ```
   huawei(config)#shdsl line-profile quickadd 10 line two-wire rate 2048 2048
   psd
   symmetric transmission Annex-A remote disable probe disable snr-margin ds-curr
   10 ds-worst
    10 us-curr 10 us-worst 10 bitmap 0x03
   ```

2. Configure the SHDSL alarm profile.

   To configure the SHDSL alarm profile, run the **shdsl alarm-profile add** command.

   In this example, the default profile (profile 1) is used.

3. Configure the SHDSL traffic profile.

   To configure the SHDSL traffic profile, run the **traffic table ip** command.

   In this example, the default profile (profile 1) is used.

4. Activate the SHDSL port.

   ```
   huawei(config)#interface shl 0/5
   huawei(config-if-shl-0/5)#deactivate all
   huawei(config-if-shl-0/5)#alarm-config all 1
   huawei(config-if-shl-0/5)#activate all 10
   huawei(config-if-shl-0/5)#quit
   ```

5. Configure the upstream port.

   The SHDSL users of MA5600T/MA5603T/MA5608T-4 adopt the PPPoE authentication. In this case, the smart VLAN is used to identify the users.

   ```
   huawei(config)#vlan 3040 smart
   huawei(config)#port vlan 3040 0/19 0
   ```

6. Add the service port.

   Ports 0-15 in slot 0/5 provide the SHDSL service. To add service ports in batches, run the **multi-service-port** command.

   ```
   huawei(config)#multi-service-port vlan 3040 port 0/5 0-15 vpi 0 vci 35
   rx-cttr 6 tx-cttr 6
   ```

Step 9 Configure the GPON service.

1. Configure the service VLAN and the upstream port.

   ```
   huawei(config)#vlan 1530 smart
   huawei(config)#port vlan 1530 0/19 0
   ```

2. Configure the DBA profile.

   ```
   huawei(config)#dba-profile add profile-id 10 type1 fix 102400
   ```

3. Configure the alarm threshold profile.

   - When you need to configure the alarm threshold value to monitor the performance statistics of the activated ONT line, run the **gpon alarm-profile add** command to configure the GPON alarm threshold profile.
   - In the default GPON alarm threshold profile 1, all alarm thresholds are set to 0, which indicates that no alarm is reported.
   - In this example, the default alarm threshold profile is used. You do not need to configure it.

4. Configure the GPON traffic profile.

   ```
   huawei(config)#traffic table ip index 8 cir 10240 priority 0 priority-policy
   tag-In-Package
   ```


Copyright © Huawei Technologies Co., Ltd.

5. Add an ONT.

   NOTE

   - You can add an ONT in two ways: run the **ont add** command to add an ONT offline or run the **ont confirm** command to confirm an ONT that is in the auto-find state.
   - You need to run the **port ont-auto-find** command in the GPON mode to enable the auto-find function of the ONT.

   ```
   huawei(config)#interface gpon 0/18
   huawei(config-if-gpon-0/18)#ont add 1 sn-auth hwhw-10101010 profile-id 2
   ```

   NOTE

   In this example, the ONT uses the default capability set profile 2. You can run the **ont-profile add** command to configure the capability set profile of the ONT based on your requirements.

6. Bind the alarm threshold profile.

   ```
   huawei(config-if-gpon-0/18)#ont alarm-profile 1 0 profile-id 1
   ```

7. Bind the DBA profile.

   ```
   huawei(config-if-gpon-0/18)#tcont bind-profile 1 0 1 profile-id 10
   ```

8. Divide the ONT port VLAN.

   ```
   huawei(config-if-gpon-0/18)#ont port vlan 1 0 eth 10 0
   huawei(config-if-gpon-0/18)#ont port native-vlan 1 0 eth 0 vlan 1530
   ```

9. Configure the GEM port.

   ```
   huawei(config-if-gpon-0/18)#gemport add 1 gemportid 150 eth
   ```

10. Bind the GEM port to an ONT T-CONT.

    NOTE

    In the actual application, if the ONT terminal does not support the priority queue scheduling, you can use the CAR to limit the rate when binding the GEM port to the ONT T-CONT.

    ```
    huawei(config-if-gpon-0/18)#ont gemport bind 1 0 150 1 priority-queue 3
    ```

11. Create the mapping between the GEM port and the service stream.

    ```
    huawei(config-if-gpon-0/18)#ont gemport mapping 1 0 150 vlan 1530
    huawei(config-if-gpon-0/18)#quit
    ```

12. Add the service port.

    ```
    huawei(config)#service-port vlan 1530 gpon 0/18/0 gemport 150 multi-service
     user-vlan 10 rx-cttr 5 tx-cttr 8
    ```

Step 10 Configure the POTS service.

1. Configure the upstream ports of the media stream and the signaling flow.

   ```
   huawei(config)#vlan 1600 smart
   huawei(config)#port vlan 1600 0/19 0
   huawei(config)#interface vlanif 1600
   huawei(config-if-vlanif1600)#ip address 10.176.6.33 24
   huawei(config-if-vlanif1600)#quit
   ```

2. Configure the static route destined to the MGC.

   NOTE

   When the MGC and the MG are in the same network segment, you do not need to configure the static route.

   ```
   huawei(config)#ip route-static 10.30.80.0 255.255.255.0 10.176.6.62
   ```

3. Configure the media IP address pool and the signaling IP address pool.

   ```
   huawei(config)#voip
   huawei(config-voip)#ip address media 10.176.6.33 10.176.6.62
   huawei(config-voip)#ip address signaling 10.176.6.33
   huawei(config-voip)#quit
   ```


Copyright © Huawei Technologies Co., Ltd.

4. Configure the MG interface.

   Add an MG interface.

   ```
   huawei(config)#interface h248 0
     Are you sure to add MG interface? (y/n)[n]:y
   ```

   Configure the MG interface attributes.

   ```
   huawei(config-if-h248-0)#if-h248 attribute mgip 10.176.6.33 mgport 2944 code
   text
    transfer udp primary-mgc-ip1 10.30.80.65 primary-mgc-port 2944 mg-media-ip1
   10.176.6.33
   ```

   Configure the software parameters of the MG interface (in this example, only parameter 20 is configured, and other parameters use the default values).

   ```
   huawei(config-if-h248-0)#mg-software parameter 20 2
   ```

5. Reset the MG interface.

   NOTE

   After configuring the MG interface, you need to reset the interface to validate the configuration.

   ```
   huawei(config-if-h248-0)#reset coldstart
     Are you sure to reset MG interface?(y/n)[n]:y
   huawei(config-if-h248-0)#quit
   ```

6. Configure the data of PSTN user.

   ```
   huawei(config)#esl user
   huawei(config-esl-user)#mgpstnuser batadd 0/3/0 0/3/31 0 terminalid 0 telno
   88660000
   huawei(config-esl-user)#quit
   ```

Step 11 Configure the multicast service.

After the configuration, the following results should be achieved:

- Users of port 0/2/2 must be authenticated, and have rights to watch two programs and to preview one program.
- Users of port 0/2/3 do not need authenticating.

1. Configure the xDSL.

   In this example, it is unnecessary to configure the xDSL. The default line profile (profile 1002) is used.

2. Configure the VLAN.

   - Create a smart VLAN.
     ```
     huawei(config)#vlan 100 smart
     ```
   - Set the VLAN upstream port.
     ```
     huawei(config)#port vlan 100 0/19 0
     ```
   - Configure the native VLAN.
     ```
     huawei(config)#interface giu 0/19
     huawei(config-if-giu-0/19)#native-vlan 0 vlan 100
     huawei(config-if-giu-0/19)#quit
     ```
   - Create a traffic profile.
     ```
     huawei(config)#traffic table ip index 8 cir off priority 5 priority-policy
     local-Setting
     ```
   - Add ADSL2+ ports 2 and port 3 to VLAN 100.
     ```
     huawei(config)#service-port vlan 100 adsl 0/2/2 vpi 0 vci 35 rx-cttr 8
     tx-cttr 8
     huawei(config)#service-port vlan 100 adsl 0/2/3 vpi 0 vci 35 rx-cttr 8
     tx-cttr 8
     ```


Copyright © Huawei Technologies Co., Ltd.

3. Configure the multicast service.

   - Enable the multicast proxy function.

     ```
     huawei(config)#multicast-vlan 100
     huawei(config-mvlan100)#igmp mode proxy
       Are you sure to change IGMP mode?(y/n)[n]:y
     ```

   - Add the upstream port.

     ```
     huawei(config-mvlan100)#igmp uplink-port 0/19/0
     huawei(config-mvlan100)#quit
     huawei(config)#btv
     huawei(config-btv)#igmp uplink-port-mode mstp
     Are you sure to change the uplink port mode?(y/n)[n]:y
     ```

   - Configure the preview parameters.

     In this example, configure the preview authority profile with the preview duration for the program to 150s, the number of preview attempts to 6 each day, and the preview interval to 60s.

     ```
     huawei(config-btv)#igmp preview-profile add index 1 duration 150 times 6
     interval 60
     huawei(config-btv)#igmp preview auto-reset-time 00:00:00
     huawei(config-btv)#quit
     ```

   - Configure the program library.

     ```
     huawei(config)#multicast-vlan 100
     huawei(config-mvlan100)#igmp program add name program1 ip 224.1.1.1
     sourceip 10.10.10.10
     huawei(config-mvlan100)#igmp program add name program2 ip 224.1.1.2
     sourceip 10.10.10.10
     huawei(config-mvlan100)#igmp program add name program3 ip 224.1.1.3
     sourceip 10.10.10.10 preview-profile 1
     huawei(config-mvlan100)#quit
     ```

   - Configure the authority profile.

     ```
     huawei(config)#btv
     huawei(config-btv)#igmp profile profile-name profile0 program-name program1
     watch
     huawei(config-btv)#igmp profile profile-name profile0 program-name program2
     watch
     huawei(config-btv)#igmp profile profile-name profile0 program-name program3
     preview
     ```

   - Configure the user data.

     ```
     huawei(config-btv)#igmp user add port 0/2/3 adsl 0 35 no-auth
     huawei(config-btv)#igmp user add port 0/2/2 adsl 0 35 auth
     huawei(config-btv)#igmp user bind-profile port 0/2/2 profile-name profile0
     huawei(config-btv)#quit
     huawei(config)#multicast-vlan 100
     huawei(config-mvlan100)#igmp multicast-vlan member port 0/2/2
     huawei(config-mvlan100)#igmp multicast-vlan member port 0/2/3
     huawei(config-mvlan100)#quit
     ```

Step 12 Save the data.

```
huawei(config)#save
```

----End

5.7 Configuring MA5600T/MA5603T/MA5608T-5

This topic describes how to configure MA5600T/MA5603T/MA5608T-5.

Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Confirm the board.

```
huawei>enable
huawei#config
huawei(config)#board confirm 0
```

Step 2 Configure the NMS.

1. Configure the IP address of the inband NMS interface.
   - Create the NMS VLAN.
     ```
     huawei(config)#vlan 10 standard
     ```
   - Add the upstream port.
     ```
     huawei(config)#port vlan 10 0/19 0
     ```
   - Enter the NMS VLAN interface mode.
     ```
     huawei(config)#interface vlanif 10
     ```
   - Configure the IP address of the NMS VLAN interface.
     ```
     huawei(config-if-vlanif10)#ip address 10.10.1.6 255.255.255.0
     huawei(config-if-vlanif10)#quit
     ```
2. Add the route.
   - Configure the route destined to the NMS (trap destination host).
     ```
     huawei(config)#ip route-static 2.2.2.2 255.255.255.255 10.10.1.1
     preference 1
     ```
   - Configure the route destined to the time server.
     ```
     huawei(config)#ip route-static 4.4.4.4 255.255.255.255 10.10.1.1
     preference 1
     ```
   - Configure the route destined to the log host.
     ```
     huawei(config)#ip route-static 3.3.3.3 255.255.255.255 10.10.1.1
     preference 1
     huawei(config)#ip route-static 3.3.4.3 255.255.255.255 10.10.1.1
     preference 1
     ```
3. Add the ACL rule.
   ```
   huawei(config)#acl 3050
   huawei(config-acl-adv-3050)#rule permit ip source any destination any
   huawei(config-acl-adv-3050)#rule deny ip source any destination 10.10.1.2
   0.0.0.0
   huawei(config-acl-adv-3050)#rule permit ip source 2.2.2.2 0.0.0.0
   destination 10.10.1.2 0.0.0.0
   huawei(config-acl-adv-3050)#rule permit ip source 2.2.2.3 0.0.0.0
   destination 10.10.1.2 0.0.0.0
   huawei(config-acl-adv-3050)#rule permit ip source 4.4.4.4 0.0.0.0
   destination 10.10.1.2 0.0.0.0
   huawei(config-acl-adv-3050)#rule permit ip source 4.4.4.5 0.0.0.0
   destination 10.10.1.2 0.0.0.0
   huawei(config-acl-adv-3050)#rule permit ip source 3.3.3.3 0.0.0.0
   destination 10.10.1.2 0.0.0.0
   huawei(config-acl-adv-3050)#rule permit ip source 3.3.4.3 0.0.0.0
   destination 10.10.1.2 0.0.0.0
   huawei(config-acl-adv-3050)#quit
   huawei(config)#packet-filter inbound ip-group 3050 port 0/19/0
   huawei(config)#packet-filter inbound ip-group 3050 port 0/19/1
   ```
4. Configure SNMP.
   - Configure the community name and access authority.
     ```
     huawei(config)#snmp-agent community read public
     huawei(config)#snmp-agent community write private
     ```
   - Configure the contact information.
     ```
     huawei(config)#snmp-agent sys-info contact HW-075512345678
     ```


Copyright © Huawei Technologies Co., Ltd.

- Configure the device local information.
  ```
  huawei(config)#snmp-agent sys-info location Shenzhen China
  ```
- Configure the SNMP version.

  The SNMP version must be the same as the SNMP version of the NMS. In this example, the NMS version is set as SNMP V2C.

  ```
  huawei(config)#snmp-agent sys-info version v2c
  ```

5. Enable the trap sending.
   ```
   huawei(config)#snmp-agent trap enable standard
   ```
6. Set the trap destination address.
   ```
   huawei(config)#snmp-agent target-host trap-hostname huawei address 2.2.2.2
   trap-paramsname abc
   huawei(config)#snmp-agent target-host trap-hostname huawei123 address 2.2.2.3
   trap-paramsname 123
   ```
7. Set the trap source address.
   ```
   huawei(config)#snmp-agent trap source vlanif 10
   ```

Step 3 Configure the time server.

```
huawei(config)#ntp-service unicast-server 4.4.4.4 source-interface vlanif 10
huawei(config)#ntp-service unicast-server 4.4.4.5 source-interface vlanif 10
```

Step 4 Configure the log host.

```
huawei(config)#loghost add 3.3.3.3 syslog-1
huawei(config)#loghost activate ip 3.3.3.3
huawei(config)#loghost add 3.3.4.3 syslog-2
huawei(config)#loghost activate ip 3.3.4.3
```

Step 5 Configure the EMU.

This topic uses the fan and the PS4875L power supply as an example to describe how to configure the EMU.

By default, the default slave node number of the fan EMU is 0. In this example, assume that the slave node number is 1. In this case, you need to set the DIP switch of the node address on the fan monitoring unit as 1.

```
huawei(config)#emu add 0 power4875l 0 0
huawei(config)#emu add 1 fan 0 1
huawei(config)#interface emu 0
huawei(config-if-power4875l-0)#power module-num 2 1 2
huawei(config-if-power4875l-0)#quit
```

Step 6 Configure the VDSL2 service.

The MA5600T/MA5603T/MA5608T supports the VDSL2 Internet service of multiple encapsulation modes, such as IPoA, PPPoA, IPoE, and PPPoE. This topic uses the PPPoE mode as an example to describe how to configure the VDSL2 service. For other encapsulation modes, see "**3.1 Example: Configuring the xDSL Internet Access Service**."

1. Configure the VDSL2 line profile.

   You can configure the VDSL2 line profile based on your requirements.

   ```
   huawei(config)#vdsl line-profile add 10
     Start adding
   profile
     Press 'Q' to quit the current configuration and new configuration will
   be
   neglected
   >  Do you want to name the profile (y/n)
   [n]:
   ```


Copyright © Huawei Technologies Co., Ltd.

```
>    Transmission
mode:
>      0:
Custom
>      1: All (G.992.1~5,T1.413,G.
993.2)
>      2: Full rate(G.992.1/3/5,T1.413,G.
993.2)
>      3: G.DMT (G.992.1/3/5,G.
993.2)
>      4: G.HS (G.992.1~5,G.
993.2)
>      5: ADSL (G.
992.1~5,T1.413)
>      6: VDSL (G.
993.2)
>    Please select (0~6)
[1]:
>  Bit swap downstream 1-disable 2-enable (1~2)
[2]:
>  Bit swap upstream   1-disable 2-enable (1~2)
[2]:
>  Please select the form of transmit rate adaptation
downstream:
>  1-fixed, 2-adaptAtStartup, 3-adaptAtRuntime (1~3)
[2]:
>  Please select the form of transmit rate adaptation
upstream:
>  1-fixed, 2-adaptAtStartup, 3-adaptAtRuntime (1~3)
[2]:
>  Will you set SNR margin parameters? (y/n)
[n]:
>  Will you set DPBO parameters? (y/n)
[n]:
>  Will you set UPBO parameters? (y/n)
[n]:
>  Will you set power management parameters? (y/n)
[n]:
>  Will you set RFI notch configuration parameter? (y/n)
[n]:
>  Will you set ADSL tone blackout configuration parameter? (y/n)
[n]:
>  Will you set VDSL tone blackout configuration parameter? (y/n)
[n]:
>  Will you set mode-specific parameters? (y/n)
[n]:
>  Will you set network timing reference? (y/n)
[n]:
>  Will you set INM parameter? (y/n)
[n]:
>  Will you set SOS downstream parameter? (y/n)
[n]:
>  Will you set SOS upstream parameter? (y/n)
[n]:
  Add profile 10 successfully
```

2. Configure the VDSL2 channel profile.

   You can configure the VDSL2 channel profile based on your requirements.

```
huawei(config)#vdsl channel-profile add 10
  Start adding
profile
  Press 'Q' to quit the current configuration and new configuration will
be
neglected
>  Do you want to name the profile (y/n)
[n]:
>  Data path mode 1-ATM, 2-PTM, 3-Both (1~3) [3]:
```


Copyright © Huawei Technologies Co., Ltd.

```
1
>  Will you set the minimum impulse noise protection? (y/n)
[n]:y
>    Minimum impulse noise protection
downstream:
>    1-noProtection    2-halfSymbol      3-singleSymbol     4-
twoSymbols
>    5-threeSymbols    6-fourSymbols     7-fiveSymbols      8-
sixSymbols
>    9-sevenSymbols    10-eightSymbols   11-nineSymbols     12-
tenSymbols
>    13-elevenSymbols  14-twelveSymbols  15-thirteenSymbols 16-
fourteenSymbols
>    17-fifteenSymbols 18-
sixteenSymbols
>    Please select (1~18) [1]:
3
>    Minimum impulse noise protection
upstream:
>    1-noProtection    2-halfSymbol      3-singleSymbol     4-
twoSymbols
>    5-threeSymbols    6-fourSymbols     7-fiveSymbols      8-
sixSymbols
>    9-sevenSymbols    10-eightSymbols   11-nineSymbols     12-
tenSymbols
>    13-elevenSymbols  14-twelveSymbols  15-thirteenSymbols 16-
fourteenSymbols
>    17-fifteenSymbols 18-
sixteenSymbols
>    Please select (1~18) [1]:
3
>  Will you set interleaving delay parameters? (y/n)
[n]:y
>    Maximum interleaving delay downstream (0~200 ms)
[20]:
>    Maximum interleaving delay upstream (0~200 ms)
[20]:
>  Will you set parameters for rate? (y/n)
[n]:y
>    Minimum transmit rate downstream (64~100000 Kbps)
[64]:
>    Minimum reserved transmit rate downstream (64~100000 Kbps)
[64]:
>    Maximum transmit rate downstream (64~100000 Kbps)
[100000]:
>    Minimum transmit rate upstream (64~100000 Kbps)
[64]:
>    Minimum reserved transmit rate upstream (64~100000 Kbps)
[64]:
>    Maximum transmit rate upstream (64~100000 Kbps)
[100000]:
>  Will you set rate thresholds? (y/n)
[n]:
>  Will you set retransmission function (y/n)
[n]:
>  Will you set erasure decoding? (y/n)
[n]:
>  Will you set SOS bit rate (y/n) [n]:
  Add profile 10 successfully
```

3. Configure the VDSL2 line template.

   Bind the preceding configured line profile and the channel profile together in the line template with the index of 10.

```
huawei(config)#vdsl line-template add 10
  Start adding template
  Press 'Q' to quit the current configuration and new configuration will be
```


Copyright © Huawei Technologies Co., Ltd.

```
neglected
>  Do you want to name the template (y/n) [n]:
>  Please set the line-profile index (1~128) [1]:10
>  Will you set channel configuration parameters? (y/n) [n]:y
>    Please set the channel number (1~2) [1]:
>    Channel1 configuration parameters:
>    Please set the channel-profile index (1~128) [1]:10
  Add template 10 successfully
```

4. Configure the VDSL2 alarm profile.

   You can configure the VDSL2 alarm profile based on your requirements. For the configuration, see "Configuring a VDSL2 Alarm Template." In this example, the default alarm profile 1 is used.

5. Configure the VDSL2 traffic profile.

   You can configure the VDSL2 traffic profile by running the **traffic table ip** command based on your requirements.

   In this example, the default profile (profile 6) is used.

6. Activate the VDSL2 port.

```
huawei(config)#interface vdsl 0/2
huawei(config-if-vdsl-0/2)#alarm-config all
huawei(config-if-vdsl-0/2)#activate all template-index 10
huawei(config-if-vdsl-0/2)#quit
```

7. Configure the upstream port.

   - Configure the GIU board.

     In general, the GE optical port uses the default gigabit full-duplex mode.
     To change the mode, switch to the GIU config mode. Then run the **speed** command to change the port rate, and run the **duplex** command to change the port duplex mode.
     The settings of the upstream port must be the same as the settings on the peer device.

   - Configure the VLAN.

     The VDSL2 users of MA5600T/MA5603T/MA5608T-1 use the PPPoE authentication. In this case, the smart VLAN is used to identify the users.

```
huawei(config)#vlan 1800 smart
huawei(config)#port vlan 1800 0/19 0
```

8. Add the service port.

   All ports in slot 0/2 provide the VDSL2 Internet access service. To add service ports in batches, run the **multi-service-port** command.

```
huawei(config)#multi-service-port vlan 1800 port 0/2 0-23 vpi 0 vci 35
 user-encap pppoe rx-cttr 6 tx-cttr 6
```

Step 7 Configure the QinQ private line service.

MA5600T/MA5603T/MA5608T-1 and MA5600T/MA5603T/MA5608T-5 serve two branches of a company to provide the QinQ private line service.

1. Create VLAN 50.

```
huawei(config)#vlan 50 mux
```

2. Set VLAN50 as QinQ VLAN.

```
huawei(config)#vlan attrib 50 q-in-q
```

3. Add the upstream port.

```
huawei(config)#port vlan 50 0/19 0
```


Copyright © Huawei Technologies Co., Ltd.

4. Add the service port.

   To add the service port, run the **service-port** command. Note that the VPI and VCI values set during the execution of the **service-port** command must be the same as those on the modem.

   The QinQ VLAN supports the PVC-priority scheduling policy only. In this case, select the profile that supports PVC-priority policy.

   ```
   huawei(config)#traffic table ip index 7 cir off priority 0 priority-policy
   local-Setting
   huawei(config)#service-port vlan 50 shdsl mode atm 0/5/15 vpi 0 vci 35 rx-cttr
   7 tx-cttr 7
   ```

Step 8 Save the data.

```
huawei(config)#save
```

----End

5.8 Verification

All services configured on all DSLAMs run in the normal state.

Copyright © Huawei Technologies Co., Ltd.

6 Configuration Example of VPLS

About This Chapter

Virtual private LAN service (VPLS) enables geographically isolated users (individuals or branch offices of an enterprise) to establish point-to-multipoint connections between each other using Ethernet links, achieving fast and flexible service deployment.

Prerequisites

Only the SPUB board supports the VPLS.

Context

As a combination of Ethernet and Multiprotocol Label Switching (MPLS) technologies, VPLS emulates all functions of the traditional local area network (LAN), with a purpose to connect multiple geographically isolated LANs that consist of Ethernet using the IP or MPLS network provided by carriers and make the LANs work as a LAN.

Currently, the MA5600T/MA5603T/MA5608T only supports Label Distribution Protocol (LDP)-based VPLS.

Table 6-1 provides basic concepts of VPLS.

Table 6-1 Basic concepts of VPLS

Concept	Description
VSI	Virtual switch instance. This concept corresponds to virtual local area network (VLAN) of Ethernet switch. Each VSI provides independent VPLS service. VSI supports the Ethernet bridge function and can terminate PW.

Copyright © Huawei Technologies Co., Ltd.

Concept	Description
PW	Pseudo wire. PW is a virtual connection between two PEs and transmits frames between the PEs. PEs use signaling to establish PWs and maintain PW status. On a VPLS network, PE routers transmit signaling to each other to establish PWs of full interconnection. Signaling exchange modes are as follows: ● Martini mode: In this mode, signaling is exchanged using the LDP protocol. This mode does not support the PE automatic discovery function. PEs need to be configured manually. With this mode, the networking is simple, and low requirements are imposed on PEs which do not need to cross domains. ● Kompella mode: Signaling is exchanged using the Border Gateway Protocol (BGP). The MA5600T/MA5603T/MA5608T does not support this mode.
AC	Attachment circuit. AC attaches a CE to a PE. An AC can be a physical or logical link. It transmits frames between the CE and PE.
Split horizon	Split horizon is a technology that prevents route loops and speeds up route convergence. In a VPLS network, full mesh and split horizon are used to prevent loops. Split horizon in VPLS means that the data packets received from the PW at the PSN side are not forwarded to other PWs. Instead, they are forwarded to the private network.

6.1 Configuration Example of the VPLS Internet Access Service
This topic describes how to configure the Internet access service for individual users when the VPLS networking is used at the access and aggregation layers.

6.2 Configuration Example of the VPLS Multicast Service
In the networking for multicast services, VPLS deployed on the MA5600T/MA5603T/MA5608T enables the MA5600T/MA5603T/MA5608T to be dual homed to AGS devices (aggregation switches), which ensures network reliability.

6.3 Configuration Example of the VPLS Enterprise Private Line Service
This topic describes how to configure the enterprise private line service when the VPLS networking is used at the access and aggregation layers.

Copyright © Huawei Technologies Co., Ltd.

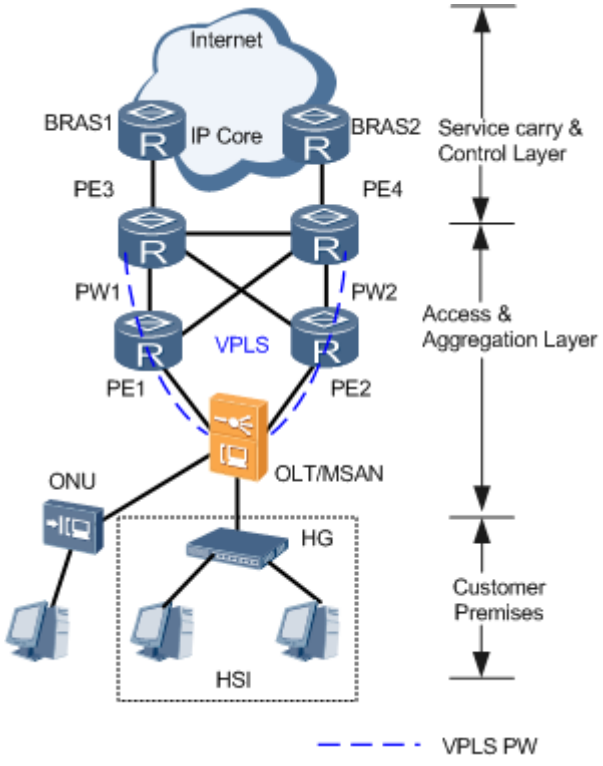
6.1 Configuration Example of the VPLS Internet Access Service

This topic describes how to configure the Internet access service for individual users when the VPLS networking is used at the access and aggregation layers.

Application Context

As shown in **Figure 6-1**, the MA5600T/MA5603T/MA5608T is dual homed to two AGS devices (aggregation switches) PE3 and PE4 through VPLS, and the Internet access service is received in PPPoE dialup mode. In the upstream direction, the traffic stream is mapped into the VPLS domain through VLAN. The PPPOE active discovery initiation (PADI) packets initiated by the user are broadcast in the VPLS domain it belongs to, and then the broadcast packets are received by the two AGS devices. The AGS devices terminate packets of some users respectively in delay response mode to achieve load sharing. When a BRAS device is faulty, the user dials up again. Then the VPLS MAC learning and forwarding mechanism automatically selects a new BRAS to provide services.

Figure 6-1 Networking for the VPLS Internet access service for individual users



Prerequisite

Traffic streams have been configured on the MA5600T/MA5603T/MA5608T for the Internet access service.

Copyright © Huawei Technologies Co., Ltd.

NOTE

To configure the Internet access service, you must configure SVLAN 100-based traffic streams on the MA5600T/MA5603T/MA5608T and perform corresponding configurations on the HG. The configurations are the same as those for common Internet access service, which are not described here.

Data Plan

Table 6-2 provides the key data plan for the MA5600T/MA5603T/MA5608T.

Table 6-2 Key data plan

Configuration Item	Data	Remarks	Requirement on PE3 and PE4
MPLS	● LSR ID: 10.10.10.10 ● VLAN: 4001	MPLS must be enabled at three layers. ● MPLS must be enabled globally. ● MPLS must be enabled for VLAN. ● MPLS must be enabled at VLAN interfaces.	The LSR ID must be unique on the entire network and MPLS must be enabled.
LDP	● MPLS LDP is enabled. ● Split horizon is enabled.	MPLS LDP must be enabled at three layers. ● MPLS LDP must be enabled globally. ● MPLS LDP must be enabled at VLAN interfaces.	MPLS LDP is enabled. The remote LDP session to the MA5600T/MA5603T/MA5608T is configured on PE3 and PE4.
Routing protocol	The Open Shortest Path First (OSPF) protocol is used.	Ensure that the Layer 3 interfaces on the MA5600T/MA5603T/MA5608T and those on PE3 and PE4 can ping each other.	Layer 3 interfaces and routes are configured on PE3 and PE4. Ensure that the Layer 3 interfaces and LSR IDs on PE3 and PE4 and those on the MA5600T/MA5603T/MA5608T can ping each other.
VPLS PW	● PW ID: 1 and 2 ● Service type: vpls ● Encapsulation type: ethernet tagged ● The control word is enabled.	On the MA5600T/MA5603T/MA5608T, PW1 and PW2 are created for PE3 and PE4 respectively. In this way, packets can be transmitted to BRAS devices over two trails.	The LDP VPLS is supported. VPLS PWs to the MA5600T/MA5603T/MA5608T are configured on PE3 and PE4, and attributes of PWs are consistent with those on the MA5600T/MA5603T/MA5608T.

Copyright © Huawei Technologies Co., Ltd.

Configuration Item	Data	Remarks	Requirement on PE3 and PE4
VSI	● PW1 and PW2 are bound to VSI. ● VLAN 100 of the Internet access service is bound to VSI.	VSI binds VLAN and PW to map VLAN to the VPLS domain, so that PADI packets for the Internet access service can be broadcast in the VPLS domain at first, until one of the BRAS response.	VSI is configured on PE3 and PE4 and the VSI ID must bind the corresponding PW.

Procedure

Step 1 Configure the basic MPLS.

1. Configure a loopback interface.

   Set the ID of the loopback interface to **0** and its IP address to **10.10.10.10/32**.

   ```
   huawei(config)#interface loopback 0
   huawei(config-if-loopback0)#ip address 10.10.10.10 32
   huawei(config-if-loopback0)#quit
   ```

2. Configure the MPLS LSR-ID. Use the IP address of loopback interface 0 as the LSR ID.

   ```
   huawei(config)#mpls lsr-id 10.10.10.10
   ```

3. Enable MPLS globally.

   Trigger LDP by the IP address of the host to set up an LSP.

   ```
   huawei(config)#mpls
   huawei(config-mpls)#lsp-trigger host
   huawei(config-mpls)#quit
   ```

4. Enable the L2VPN function.

   ```
   huawei(config)#mpls l2vpn
   ```

5. Enable the LDP function globally and enable the split horizon policy.

   ```
   huawei(config)#mpls ldp
   huawei(config-mpls-ldp)#outbound peer all split-horizon
   huawei(config-mpls-ldp)#quit
   ```

Step 2 Configure VLAN and enable MPLS for VLAN and VLAN interfaces.

1. Add VLAN 4001 for forwarding MPLS packets and add upstream port 0/19/0 and 0/19/1 to it.

   ```
   huawei(config)#vlan 4001 smart
   huawei(config)#port vlan 4001 0/19/0
   huawei(config)#port vlan 4001 0/19/1
   ```

2. Enable MPLS for VLAN 4001.

   ```
   huawei(config)#mpls vlan 4001
   ```

3. Set the IP address of VLAN interface 4001 to **10.50.50.50/24** and enable MPLS LDP for the VLAN interface.

   ```
   huawei(config)#interface vlanif 4001
   huawei(config-if-vlanif4001)#ip address 10.50.50.50 24
   huawei(config-if-vlanif4001)#mpls
   ```


Copyright © Huawei Technologies Co., Ltd.

```
huawei(config-if-vlanif4001)#mpls ldp
huawei(config-if-vlanif4001)#quit
```

Step 3 Configure routes.

VPLS has no special requirements on routing policy. You can use static route, RIP, or OSPF policy. In the following example, OSPF is used.

Set the OSPF process ID to **100** and OSPF area ID to **1**. In addition, configure the interfaces (VLAN interface and loopback interface) that run OSPF and configure the areas of the interfaces.

```
huawei(config)#ospf 1
huawei(config-ospf-1)#area 100
huawei(config-ospf-1-area-0.0.0.100)#network 10.50.50.0 0.0.0.255
huawei(config-ospf-1-area-0.0.0.100)#network 10.10.10.10 0.0.0.0
huawei(config-ospf-1-area-0.0.0.100)#return
```

Step 4 Configure the remote LDP session.

Configure the remote LDP session from the MA5600T/MA5603T/MA5608T to PE3 (LSR ID: 3.3.3.3) and PE4 (LSR ID: 4.4.4.4) respectively. Name the sessions **to_pe3** and **to_pe4** respectively.

```
huawei(config)#mpls ldp remote-peer to_pe3
huawei(config-mpls-ldp-remote-to_pe3)#remote-ip 3.3.3.3
huawei(config-mpls-ldp-remote-to_pe3)#remote-ip auto-dod-request
huawei(config-mpls-ldp-remote-to_pe3)#quit
huawei(config)#mpls ldp remote-peer to_pe4
huawei(config-mpls-ldp-remote-to_pe4)#remote-ip 4.4.4.4
huawei(config-mpls-ldp-remote-to_pe4)#remote-ip auto-dod-request
huawei(config-mpls-ldp-remote-to_pe4)#quit
```

Step 5 Configure a VSI.

1. Add a VSI.

   Create a VSI named **hsi**. Set the signaling protocol to **LDP**. and VSI ID to **1**.

   ```
   huawei(config)#vsi hsi
   huawei(config-vsi-hsi)#pwsignal ldp
   huawei(config-vsi-hsi)#vsi-id 1
   ```

2. (Optional) Configure the attributes of VSI.

   Configure basic attributes of VSI as required, including the encapsulation type, control word, MTU value, and traffic suppression policy. In the following example, the control word is enabled and default values are used for other parameters.

   ```
   huawei(config-vsi-hsi)#control-word
   ```

Step 6 Configure PWs.

Create two PWs with IDs 1 and 2. Set the service type to **vpls**, remote IP addresses to **3.3.3.3** and **4.4.4.4** respectively, and encapsulation type to **ethernet tagged**. Enable the control word, and set the receive labels of dynamic PW to **10240** and **10250** respectively.

```
huawei(config)#pw-para pwindex 1
huawei(config-pw-para-index-1)#service-type vpls
huawei(config-pw-para-index-1)#pwid 1
huawei(config-pw-para-index-1)#peer-address 3.3.3.3
huawei(config-pw-para-index-1)#pw-type ethernet tagged
huawei(config-pw-para-index-1)#control-word enable
huawei(config-pw-para-index-1)#dyn-receive-label 10240
huawei(config-pw-para-index-1)#quit
huawei(config)#pw-para pwindex 2
huawei(config-pw-para-index-2)#service-type vpls
huawei(config-pw-para-index-2)#pwid 2
huawei(config-pw-para-index-2)#peer-address 4.4.4.4
huawei(config-pw-para-index-2)#pw-type ethernet tagged
huawei(config-pw-para-index-2)#control-word enable
```


Copyright © Huawei Technologies Co., Ltd.

```
huawei(config-pw-para-index-2)#dyn-receive-label 10250
huawei(config-pw-para-index-2)#quit
```

Step 7 Bind PW and VSI.

Dynamically bind PW1 and PW2 to the VSI named **hsi** to establish the VPLS PW service.

```
huawei(config)#vsi hsi
huawei(config-vsi-hsi)#vsi-pw-binding pwindex 1
huawei(config-vsi-hsi)#vsi-pw-binding pwindex 2
```

Step 8 Bind AC and VSI.

Bind VLAN 100 to the VSI named hsi, so that the Internet access service packets of VLAN 100 can be forwarded in the VSI.

```
huawei(config-vsi-hsi)#vsi-ac-binding vlan 100
```

----End

Result

1. A user performs PPPoE dialup. A PADI packet is transmitted upstream.
2. The OLT maps the PADI packet to VSI based on SVLAN carried in the packet and broadcasts the packet on two PWs. At the same time, the OLT learns user's MAC address.
3. After receiving the PADI packet, two BRAS devices respond with PPPOE active discovery offer (PADO) packets in random delay mode.
4. After receiving the PADO packets from PWs, the OLT learns the MAC address carried in the packets from PWs and forwards the packets to the user.
5. The user receives two PADO packets at different time and only responds to the first received PADO packet to establish a PPPoE session.
6. The OLT forwards subsequent PPPOE active discovery request (PADR) and PPPOE active discovery session-confirmation (PADS) packets based on learnt MAC addresses.

6.2 Configuration Example of the VPLS Multicast Service

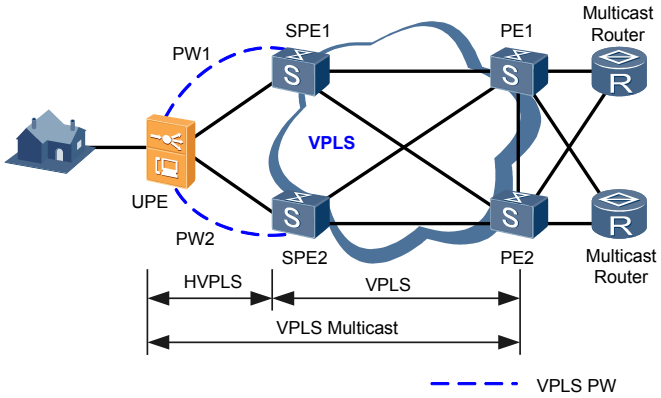
In the networking for multicast services, VPLS deployed on the MA5600T/MA5603T/MA5608T enables the MA5600T/MA5603T/MA5608T to be dual homed to AGS devices (aggregation switches), which ensures network reliability.

Application Context

In the VPLS network, multicast services are still deployed based on multicast VLAN other than based on VSI (VPLS instance). The multicast VLAN is bound to VSI for carrying multicast services over the VPLS network, including upstream IGMP packets and downstream multicast traffic streams.

Copyright © Huawei Technologies Co., Ltd.

Figure 6-2 Networking for the VPLS multicast service



As shown in **Figure 6-2**:

- The MA5600T/MA5603T/MA5608T, functioning as a UPE (underlayer PE), is located on the edge network of HVPLS. In the downstream direction, the MA5600T/MA5603T/MA5608T accesses multicast users through multicast VLAN whose IGMP mode is proxy or snooping. In the upstream direction, the MA5600T/MA5603T/MA5608T is dual homed to two AGS devices that serve as SPEs (superstratum PEs) through two PWs. The same VSI is set up on the MA5600T/MA5603T/MA5608T and AGS and the two upstream PWs belong to the VSI.
- Multiple AGS devices form a VPLS core bearer network. The AGS devices learn the VPLS multicast forwarding table and duplicate multicast traffic based on VPLS PW connections. Two edge AGS devices functioning as SPEs in the downstream direction access the UPE on the edge network, and two edge AGS devices functioning as PEs in the upstream direction terminate VPLS and are connected to multicast routers.
- Two multicast routers back up each other and import multicast traffic streams from the multicast source to the VPLS bearer network.

NOTE

Currently, a maximum of two PWs are supported for VPLS multicast services and both two PWs are used for transmitting multicast packets upstream.

Prerequisite

The MA5600T/MA5603T/MA5608T has been configured with multicast VLAN 100-based multicast traffic streams, and corresponding configurations have been performed on the HG. The configurations are similar to those for common multicast services. The difference is that multicast upstream ports do not need to be configured for VPLS multicast services and the default mode is used for the multicast upstream ports.

Data Plan

Table 6-3 provides the key data plan for the MA5600T/MA5603T/MA5608T.

Copyright © Huawei Technologies Co., Ltd.

Table 6-3 Key data plan

Configuration Item	Data	Remarks	Requirement on SPE1 and SPE2
MPLS	● LSR ID: 10.10.10.10 ● VLAN: 4001	MPLS must be enabled at three layers. ● MPLS must be enabled globally. ● MPLS must be enabled for VLAN. ● MPLS must be enabled at VLAN interfaces.	The LSR ID must be unique on the entire network and MPLS must be enabled.
LDP	● MPLS LDP is enabled. ● Split horizon is enabled.	MPLS LDP must be enabled at two layers. ● MPLS LDP must be enabled globally. ● MPLS LDP must be enabled at VLAN interfaces.	MPLS LDP is enabled. The remote LDP session to the MA5600T/MA5603T/MA5608T is configured on SPE1 and SPE2.
Routing protocol	The Open Shortest Path First (OSPF) protocol is used.	Ensure that the Layer 3 interfaces on the MA5600T/MA5603T/MA5608T and those on SPE1 and SPE2 can ping each other.	Layer 3 interfaces and routes are configured on SPE1 and SPE2. Ensure that the Layer 3 interfaces and loopback interfaces on SPE1 and SPE2 and those on the MA5600T/MA5603T/MA5608T can ping each other.
VPLS PW	● PW ID: 1 and 2 ● Service type: vpls ● Encapsulation type: ethernet tagged ● The control word is enabled.	L2VPN must be enabled. On the MA5600T/MA5603T/MA5608T, PW1 and PW2 are created for SPE1 and SPE2 respectively.	The LDP VPLS is supported. VPLS PWs to the MA5600T/MA5603T/MA5608T are configured on SPE1 and SPE2, and attributes of PWs are consistent with those on the MA5600T/MA5603T/MA5608T.
VSI	● PW1 and PW2 are bound to VSI. ● Multicast service VLAN 100 is bound to VSI.	Multicast VLAN is bound through VSI to map VLAN to the VPLS domain, so that multicast service packets can be broadcast in the VPLS domain.	VSI is configured on SPE1 and SPE2 and the VSI ID must bind the corresponding PW.

Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Configure the basic MPLS.

1. Configure a loopback interface.

   Set the ID of the loopback interface to **0** and its IP address to **10.10.10.10/32**.

   ```
   huawei(config)#interface loopback 0
   huawei(config-if-loopback0)#ip address 10.10.10.10 32
   huawei(config-if-loopback0)#quit
   ```

2. Configure the MPLS LSR-ID. Use the IP address of loopback interface 0 as the LSR ID.

   huawei(config)#**mpls lsr-id 10.10.10.10**

3. Enable MPLS globally.

   Trigger LDP by the IP address of the host to set up an LSP.

   ```
   huawei(config)#mpls
   huawei(config-mpls)#lsp-trigger host
   huawei(config-mpls)#quit
   ```

4. Enable the L2VPN function.

   ```
   huawei(config)#mpls l2vpn
   ```

5. Enable the LDP function globally and enable the split horizon policy.

   ```
   huawei(config)#mpls ldp
   huawei(config-mpls-ldp)#outbound peer all split-horizon
   huawei(config-mpls-ldp)#quit
   ```

Step 2 Configure VLAN, and enable MPLS for VLAN and VLAN interfaces.

1. Add VLAN 4001 for forwarding MPLS packets and add two upstream ports to it.

   ```
   huawei(config)#vlan 4001 smart
   huawei(config)#port vlan 4001 0/19/0
   huawei(config)#port vlan 4001 0/19/1
   ```

2. Enable MPLS for VLAN 4001.

   ```
   huawei(config)#mpls vlan 4001
   ```

3. Set the IP address of VLAN interface 4001 to **10.50.50.50/24** and enable MPLS LDP for the VLAN interface.

   ```
   huawei(config)#interface vlanif 4001
   huawei(config-if-vlanif4001)#ip address 10.50.50.50 24
   huawei(config-if-vlanif4001)#mpls
   huawei(config-if-vlanif4001)#mpls ldp
   huawei(config-if-vlanif4001)#quit
   ```

Step 3 Configure routes.

VPLS has no special requirements on routing policy. You can use static route, RIP, or OSPF policy. In the following example, OSPF is used.

Set the OSPF process ID to **100** and OSPF area ID to **1**. In addition, configure the interfaces (VLAN interface and loopback interface) that run OSPF and configure the areas of the interfaces.

```
huawei(config)#ospf 1
huawei(config-ospf-1)#area 100
huawei(config-ospf-1-area-0.0.0.100)#network 10.50.50.0 0.0.0.255
huawei(config-ospf-1-area-0.0.0.100)#network 10.10.10.10 0.0.0.0
huawei(config-ospf-1-area-0.0.0.100)#return
```

Step 4 Configure the remote LDP session.

Configure the remote LDP sessions from the MA5600T/MA5603T/MA5608T to SPE1 (LSR ID: 1.1.1.1) and SPE2 (LSR ID: 2.2.2.2) respectively. Name the sessions **to_spe1** and **to_spe2** respectively.

Copyright © Huawei Technologies Co., Ltd.

```
huawei(config)#mpls ldp remote-peer to_spe1
huawei(config-mpls-ldp-remote-to_spe1)#remote-ip 1.1.1.1
huawei(config-mpls-ldp-remote-to_spe1)#remote-ip auto-dod-request
huawei(config-mpls-ldp-remote-to_spe1)#quit
huawei(config)#mpls ldp remote-peer to_spe2
huawei(config-mpls-ldp-remote-to_spe2)#remote-ip 2.2.2.2
huawei(config-mpls-ldp-remote-to_spe2)#remote-ip auto-dod-request
huawei(config-mpls-ldp-remote-to_spe2)#quit
```

Step 5 Configure a VSI.

1. Add a VSI.

   Create a VSI named **multicast**. Set the signaling protocol to **LDP** and VSI ID to **1**.

   ```
   huawei(config)#vsi multicast
   huawei(config-vsi-multicast)#pwsignal ldp
   huawei(config-vsi-multicast)#vsi-id 1
   ```

2. (Optional) Disable the suppression of the unknown multicast of the VSI.

   If the VSI unknown multicast suppression is enabled, you need to configure this step. Otherwise, packet loss will occur in the multicast services.

   ```
   huawei(config-vsi-multicast)#undo traffic-suppress multicast
   ```

3. (Optional) Configure attributes of VSI.

   Configure basic attributes of VSI as required, including the encapsulation type, control word, and MTU value. In the following example, the control word is enabled and default values are used for other parameters.

   ```
   huawei(config-vsi-multicast)#control-word
   ```

Step 6 Configure PWs.

Create two PWs with IDs 1 and 2. Set the service type to **vpls**, the remote IP addresses to **1.1.1.1** and **2.2.2.2** respectively, and encapsulation type to **ethernet tagged**. Enable the control word, and set the receive labels of dynamic PW to **10240** and **10250** respectively.

```
huawei(config)#pw-para pwindex 1
huawei(config-pw-para-index-1)#service-type vpls
huawei(config-pw-para-index-1)#pwid 1
huawei(config-pw-para-index-1)#peer-address 1.1.1.1
huawei(config-pw-para-index-1)#pw-type ethernet tagged
huawei(config-pw-para-index-1)#control-word enable
huawei(config-pw-para-index-1)#dyn-receive-label 10240
huawei(config-pw-para-index-1)#quit
huawei(config)#pw-para pwindex 2
huawei(config-pw-para-index-2)#service-type vpls
huawei(config-pw-para-index-2)#pwid 2
huawei(config-pw-para-index-2)#peer-address 2.2.2.2
huawei(config-pw-para-index-2)#pw-type ethernet tagged
huawei(config-pw-para-index-2)#control-word enable
huawei(config-pw-para-index-2)#dyn-receive-label 10250
huawei(config-pw-para-index-2)#quit
```

Step 7 Bind PW and VSI.

Dynamically bind PW1 and PW2 to the VSI named multicast to establish the VPLS PW service.

```
huawei(config)#vsi multicast
huawei(config-vsi-multicast)#vsi-pw-binding pwindex 1
huawei(config-vsi-multicast)#vsi-pw-binding pwindex 2
```

Step 8 Bind AC and VSI.

Bind multicast VLAN 100 to the VSI named multicast, so that the multicast service packets of VLAN 100 can be forwarded in VSI.

- The same multicast VLAN cannot be bound to the VPLS instance and PW at the same time.
- The same restrictions are set for binding multicast VLANs and VSI as those for binding unicast VLANs and VSI. That is, when the VPLS encapsulation type is raw, one VIS can

Copyright © Huawei Technologies Co., Ltd.

only be bound to a multicast VLAN; when the VPLS encapsulation type is tag, one VSI can be bound to multiple multicast VLANs.

```
huawei(config-vsi-multicast)#vsi-ac-binding vlan 100
```

----End

Result

1. A user orders a multicast program. An IGMP packet is transmitted upstream.
2. The MA5600T/MA5603T/MA5608T broadcasts the IGMP packet over two upstream PWs which serve as the multicast upstream ports of the multicast VLAN.
3. On the AGS devices, VPLS exchange is performed on the IGMP packet. The AGS devices learn the VPLS multicast forwarding table and duplicate multicast traffic based on VPLS PW connections.
4. Finally, multicast traffic streams are transmitted over one PW. The MA5600T/MA5603T/MA5608T forwards the multicast traffic streams to the corresponding user port based on the local multicast forwarding table. Then the user can watch the multicast program normally.

6.3 Configuration Example of the VPLS Enterprise Private Line Service

This topic describes how to configure the enterprise private line service when the VPLS networking is used at the access and aggregation layers.

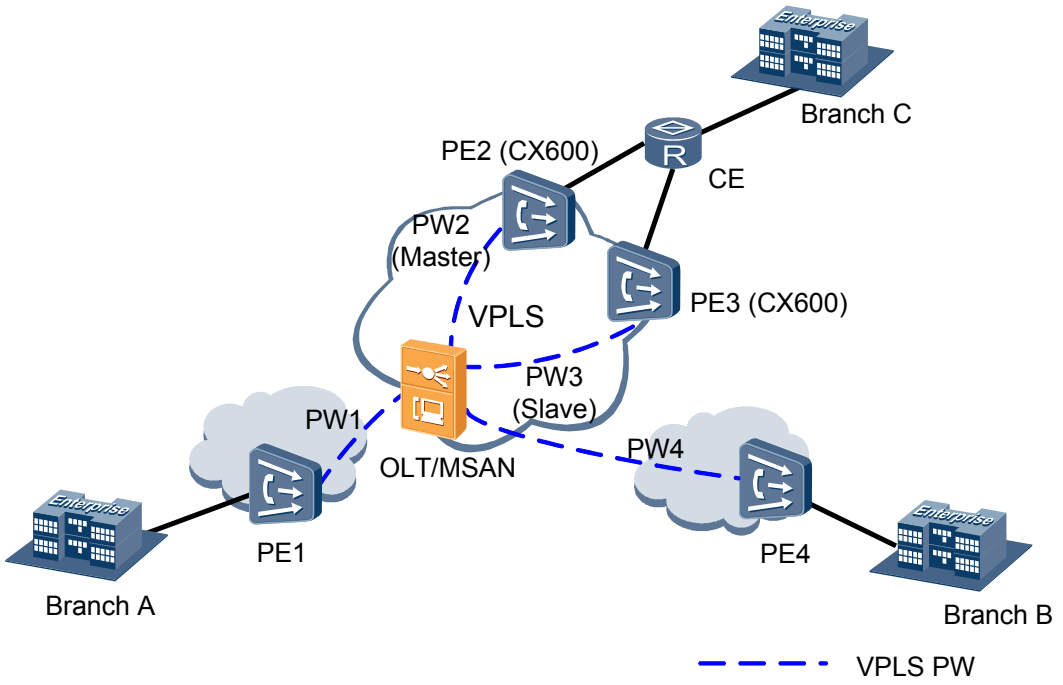
Application Context

As shown in **Figure 6-3**, branch offices of an enterprise access the VPLS network through a CE or PE. By deploying VPLS PWs between PEs, the service provider can provide Ethernet-based multipoint services to enterprise users over the MPLS backbone network and achieve emulation of the local area network (LAN). For important branch offices (for example, branch C in the following figure), PW redundancy is configured to provide protection.

In the following figure, as a key node, the OLT/MSAN (MA5600T/MA5603T/MA5608T) exchanges data with PEs (PE1-PE4) through VPLS PWs. For important branch offices, a PW protection group is configured to provide protection. PEs are connected to the OLT/MSAN using Spoke PW.

Copyright © Huawei Technologies Co., Ltd.

Figure 6-3 Networking for the VPLS enterprise private line service



Prerequisite

QinQ traffic streams have been configured on PE1-PE4 for the private line service of different branch offices.

NOTE

To configure the Ethernet-based enterprise private line service, you must configure QinQ VLAN-based Ethernet traffic streams on PE1-PE4, and perform corresponding configurations on routers for branch offices of the enterprise. The configurations are the same as those for common QinQ VLAN private line service, which are not described here.

Data Plan

Table 6-4 provides the key data plan for the OLT/MSAN (MA5600T/MA5603T/MA5608T).

Copyright © Huawei Technologies Co., Ltd.

Table 6-4 Key data plan

Configuration Item	Data	Remarks	Requirement on PE1-PE4
MPLS	● LSR ID: 10.10.10.10 ● VLAN: 4001	MPLS must be enabled at three layers. ● MPLS must be enabled globally. ● MPLS must be enabled for VLAN. ● MPLS must be enabled at VLAN interfaces.	The LSR ID must be unique on the entire network and MPLS must be enabled.
LDP	MPLS LDP is enabled.	MPLS LDP must be enabled at three layers. ● MPLS LDP must be enabled globally. ● MPLS LDP must be enabled at VLAN interfaces.	MPLS LDP is enabled. The remote LDP session to the MA5600T/MA5603T/ MA5608T is configured on PE1-PE4.
Routing protocol	The Open Shortest Path First (OSPF) protocol is used.	Ensure that the Layer 3 interfaces on the MA5600T/ MA5603T/MA5608T and those on PE1-PE4 can ping each other.	Layer 3 interfaces and routes are configured on PE1-PE4. Ensure that the Layer 3 interfaces and LSR IDs on PE1-PE4 and those on the MA5600T/MA5603T/ MA5608T can ping each other.

Copyright © Huawei Technologies Co., Ltd.

Configuration Item	Data	Remarks	Requirement on PE1-PE4
VPLS PW	● PW ID: 1, 2, 3, 4 ● Service type: vpls ● Encapsulation type: ethernet tagged ● The control word is enabled. PW protection group: ● PW ID: 2, 3 ● Working mode: master-slave ● The dual receiving function is enabled for PWs.	On the OLT/MSAN, PW1 and PW4 are created for PE1 and PE4 respectively, and PW2 and PW3 are created for PE2 and PE3 respectively. PW2 and PW3 back up each other.	The LDP VPLS is supported, and VPLS PWs to the MA5600T/MA5603T/ MA5608T are configured on PE1-PE4, and attributes of PWs are consistent with those on the MA5600T/MA5603T/ MA5608T.
VSI	● PW1-PW4 are bound to VSI. ● Binding mode of PW 1 and PW 4: spoke ● VLAN 100 of the private line service is bound to VSI.	VSI binds VLAN and PW to map VLAN to the VPLS domain, so that packets for the enterprise private line service can be broadcast in the VPLS domain.	VSI is configured on PE1-PE4 and the VSI ID must bind the corresponding PW.

Procedure

Step 1 Configure the basic MPLS.

1. Configure a loopback interface.

   Set the ID of the loopback interface to **0** and its IP address to **10.10.10.10/32**.

   ```
   huawei(config)#interface loopback 0
   huawei(config-if-loopback0)#ip address 10.10.10.10 32
   huawei(config-if-loopback0)#quit
   ```

2. Configure the MPLS LSR-ID. Use the IP address of loopback interface 0 as the LSR ID.

   ```
   huawei(config)#mpls lsr-id 10.10.10.10
   ```

3. Enable MPLS globally.

   Trigger LDP by the IP address of the host to set up an LSP.

Copyright © Huawei Technologies Co., Ltd.

```
huawei(config)#mpls
huawei(config-mpls)#lsp-trigger host
huawei(config-mpls)#quit
```

4. Enable the L2VPN function.

```
huawei(config)#mpls l2vpn
```

5. Enable LDP globally.

```
huawei(config)#mpls ldp
huawei(config-mpls-ldp)#quit
```

Step 2 Configure VLAN, and enable MPLS for VLAN and VLAN interfaces.

1. Add VLAN 4001 for forwarding MPLS packets and add four upstream ports to it.

```
huawei(config)#vlan 4001 smart
huawei(config)#port vlan 4001 0/19 0
huawei(config)#port vlan 4001 0/19 1
huawei(config)#port vlan 4001 0/20 0
huawei(config)#port vlan 4001 0/20 1
```

2. Enable MPLS for VLAN 4001.

```
huawei(config)#mpls vlan 4001
```

3. Set the IP address of VLAN interface 4001 to **10.50.50.50/24** and enable MPLS LDP for the VLAN interface.

```
huawei(config)#interface vlanif 4001
huawei(config-if-vlanif4001)#ip address 10.50.50.50 24
huawei(config-if-vlanif4001)#mpls
huawei(config-if-vlanif4001)#mpls ldp
huawei(config-if-vlanif4001)#quit
```

Step 3 Configure routes.

VPLS has no special requirements on routing policy. You can use static route, RIP, or OSPF policy. In the following example, OSPF is used.

Set the OSPF process ID to **100** and OSPF area ID to **1**. In addition, configure the interfaces (VLAN interface and loopback interface) that run OSPF and configure the areas of the interfaces.

```
huawei(config)#ospf 1
huawei(config-ospf-1)#area 100
huawei(config-ospf-1-area-0.0.0.100)#network 10.50.50.0 0.0.0.255
huawei(config-ospf-1-area-0.0.0.100)#network 10.10.10.10 0.0.0.0
huawei(config-ospf-1-area-0.0.0.100)#return
```

Step 4 Configure the remote LDP session.

Configure the remote LDP session from the MA5600T/MA5603T/MA5608T to PE1 (LSR ID: 5.5.5.5), PE2 (LSR ID: 2.2.2.2), PE3 (LSR ID: 3.3.3.3), and PE4 (LSR ID: 4.4.4.4) respectively. Name the sessions **to_pe1**, **to_pe2**, **to_pe3**, and **to_pe4** respectively.

```
huawei(config)#mpls ldp remote-peer to_pe1
huawei(config-mpls-ldp-remote-to_pe1)#remote-ip 5.5.5.5
huawei(config-mpls-ldp-remote-to_pe1)#remote-ip auto-dod-request
huawei(config-mpls-ldp-remote-to_pe1)#quit
huawei(config)#mpls ldp remote-peer to_pe2
huawei(config-mpls-ldp-remote-to_pe2)#remote-ip 2.2.2.2
huawei(config-mpls-ldp-remote-to_pe2)#remote-ip auto-dod-request
huawei(config-mpls-ldp-remote-to_pe2)#quit
huawei(config)#mpls ldp remote-peer to_pe3
huawei(config-mpls-ldp-remote-to_pe3)#remote-ip 3.3.3.3
huawei(config-mpls-ldp-remote-to_pe3)#remote-ip auto-dod-request
huawei(config-mpls-ldp-remote-to_pe3)#quit
huawei(config)#mpls ldp remote-peer to_pe4
huawei(config-mpls-ldp-remote-to_pe4)#remote-ip 4.4.4.4
huawei(config-mpls-ldp-remote-to_pe4)#remote-ip auto-dod-request
huawei(config-mpls-ldp-remote-to_pe4)#quit
```


Copyright © Huawei Technologies Co., Ltd.

Step 5 Configure VSI.

1. Add a VSI.

   Create a VSI named **enterprise_vpn**. Set the signaling protocol to **LDP** and VSI ID to **1**.

```
huawei(config)#vsi enterprise_vpn
huawei(config-vsi-enterprise_vpn)#pwsignal ldp
huawei(config-vsi-enterprise_vpn)#vsi-id 1
```

2. (Optional) Configure the attributes of VSI.

   Configure basic attributes of VSI as required, including the encapsulation type, control word, MTU value, and traffic suppression policy. In the following example, the control word is enabled and default values are used for other parameters.

```
huawei(config-vsi-enterprise_vpn)#control-word
```

Step 6 Configure PWs.

Create four PWs with IDs 1-4. Set the service type to **vpls**, the remote IP addresses to the IP addresses of PE1-PE4, and encapsulation type to **ethernet tagged**. Enable the control word, and set the receive labels of dynamic PW to **10240**, **10250**, **10260**, and **10270** respectively.

```
huawei(config)#pw-para pwindex 1
huawei(config-pw-para-index-1)#service-type vpls
huawei(config-pw-para-index-1)#pwid 1
huawei(config-pw-para-index-1)#peer-address 5.5.5.5
huawei(config-pw-para-index-1)#pw-type ethernet tagged
huawei(config-pw-para-index-1)#control-word enable
huawei(config-pw-para-index-1)#dyn-receive-label 10240
huawei(config-pw-para-index-1)#quit
huawei(config)#pw-para pwindex 2
huawei(config-pw-para-index-2)#service-type vpls
huawei(config-pw-para-index-2)#pwid 1
huawei(config-pw-para-index-2)#peer-address 2.2.2.2
huawei(config-pw-para-index-2)#pw-type ethernet tagged
huawei(config-pw-para-index-2)#control-word enable
huawei(config-pw-para-index-2)#dyn-receive-label 10250
huawei(config-pw-para-index-2)#quit
huawei(config)#pw-para pwindex 3
huawei(config-pw-para-index-3)#service-type vpls
huawei(config-pw-para-index-3)#pwid 3
huawei(config-pw-para-index-3)#peer-address 3.3.3.3
huawei(config-pw-para-index-3)#pw-type ethernet tagged
huawei(config-pw-para-index-3)#control-word enable
huawei(config-pw-para-index-3)#dyn-receive-label 10260
huawei(config-pw-para-index-3)#quit
huawei(config)#pw-para pwindex 4
huawei(config-pw-para-index-4)#service-type vpls
huawei(config-pw-para-index-4)#pwid 4
huawei(config-pw-para-index-4)#peer-address 4.4.4.4
huawei(config-pw-para-index-4)#pw-type ethernet tagged
huawei(config-pw-para-index-4)#control-word enable
huawei(config-pw-para-index-4)#dyn-receive-label 10270
huawei(config-pw-para-index-4)#quit
```

Step 7 Bind PW and VSI.

Dynamically bind PW 1 and PW 4 in spoke mode, and dynamically bind PW 2 and PW 3 to the VSI named **enterprise_vpn** to establish the VPLS PW service. The spoke mode is used to identify the peer is a user-side PE, and split horizon is not performed between PWs.

```
huawei(config)#vsi enterprise_vpn
huawei(config-vsi-enterprise_vpn)#vsi-pw-binding pwindex 1 spoke
huawei(config-vsi-enterprise_vpn)#vsi-pw-binding pwindex 2
huawei(config-vsi-enterprise_vpn)#vsi-pw-binding pwindex 3
huawei(config-vsi-enterprise_vpn)#vsi-pw-binding pwindex 4 spoke
```

Step 8 Configure VPLS PW protection.

Copyright © Huawei Technologies Co., Ltd.

Configure PW2 and PW3 as a PW protection group named **pg_pw**. Set the working mode to master-slave and enable the dual receiving function for PWs. In the protection group enabled with dual receiving, two PWs are always allowed to receive traffic. In this way, when the remote device performs traffic switching, the traffic will not be dropped.

```
huawei(config)#vsi enterprise_vpn
huawei(config-vsi-enterprise_vpn)#protect-group pg_pw
huawei(config-vsi-enterprise_vpn-group-pg_pw)#pw-protect primary-pw pwindex 2
secondary-pw pwindex 3
huawei(config-vsi-enterprise_vpn-group-pg_pw)#protect-mode master
huawei(config-vsi-enterprise_vpn-group-pg_pw)#stream-dual-receiving
```

Step 9 Bind AC and VSI.

Bind QinQ VLAN 100 to the VSI named enterprise_vpn, so that the enterprise private line service packets can be forwarded in the VSI.

```
huawei(config-vsi-enterprise_vpn)#vsi-ac-binding vlan 100
```

----End

Result

As shown in **Figure 6-3**, the private networks distributed in different branches can establish point-to-multipoint communication with each other and various services can be provisioned between these private networks. When a PE which branch C is connected to is faulty, services can be automatically switched to another PE and therefore services are not affected.

Copyright © Huawei Technologies Co., Ltd.

7 Example: Subtending Networking

About This Chapter

This topic describes how to configure the integrated services on the MA5600Ts in the multi-tier subtending network.

7.1 Subtended Network
This topic describes an example of subtended network.

7.2 Data Plan for Subtended Network
This topic describes the data plan for the example subtended network.

7.3 Configuring MA5600T-1
This topic describes how to configure MA5600T-1.

7.4 Configuring MA5600T-2
This topic describes how to configure MA5600T-2.

7.5 Configuring MA5600T-3
This topic describes how to configure MA5600T-3.

7.6 Configuring MA5600T-4
This topic describes how to configure MA5600T-4.

7.7 Verification
All services configured on all DSLAMs run in the normal state.

Copyright © Huawei Technologies Co., Ltd.

7.1 Subtended Network

This topic describes an example of subtended network.

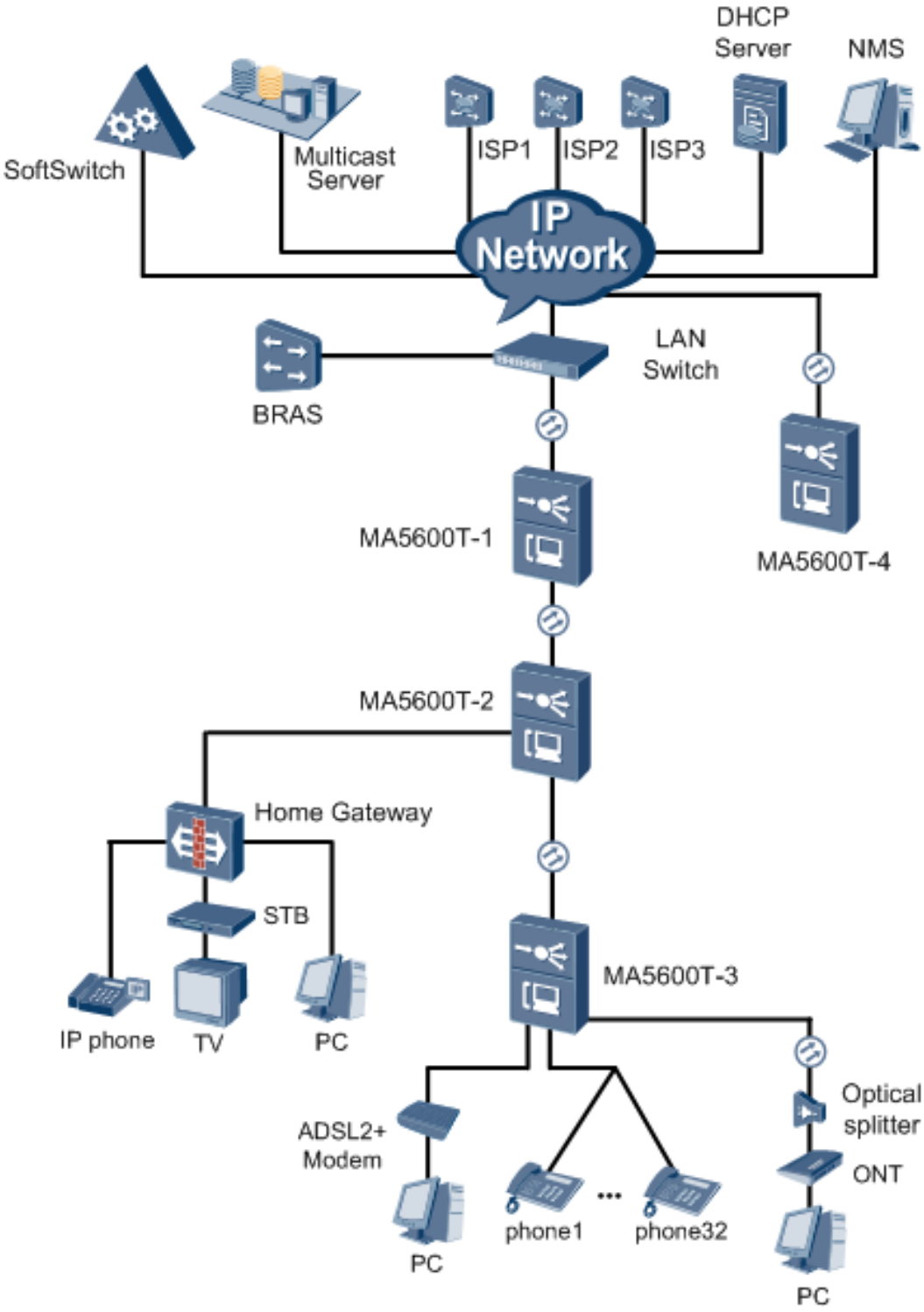
As shown in **Figure 7-1**:

- MA5600T-1 is subtended with MA5600T-2 through the GE port on the GIU board.
- MA5600T-2 is subtended with MA5600T-3 through the GE port on the GIU board.

Figure 7-1 shows an example subtended network of the MA5600T.

Copyright © Huawei Technologies Co., Ltd.

Figure 7-1 Example subtended network of the MA5600T



7.2 Data Plan for Subtended Network

This topic describes the data plan for the example subtended network.

Copyright © Huawei Technologies Co., Ltd.

Table 7-1 provides the service and the data plan for the example subtended network of the MA5600T in Figure 7-1.

Table 7-1 Data plan for the example subtended network

Item	MA5600T-1	MA5600T-2	MA5600T-3	MA5600T-4
Service	● ADSL2+ service ● SHDSL service ● GPON service ● POTS service ● QinQ private line service (for the private line interconnection withMA5600T-4) ● Multicast service	● ADSL2+ service ● SHDSL service ● POTS service ● Stacking wholesale service ● Triple play service	● ADSL2+ service ● SHDSL service ● GPON service ● POTS service ● Multicast service	● VDSL2 service ● QinQ private line service (for the private line interconnection withMA5600T-1)
Inband NMS address	10.10.1.2 255.255.255.0 Gateway: 10.10.1.1/24	10.10.1.3 255.255.255.0 Gateway: 10.10.1.1/24	10.10.1.4 255.255.255.0 Gateway: 10.10.1.1/24	10.10.1.5 255.255.255.0 Gateway: 10.10.1.1/24
GE port of the GIU board	Upstream: 0/19/0 Subtending: 0/19/1	Upstream: 0/19/0 Subtending: 0/19/1	Upstream: 0/19/0	Upstream: 0/19/0

Copyright © Huawei Technologies Co., Ltd.

Item	MA5600T-1	MA5600T-2	MA5600T-3	MA5600T-4
VLAN	NMS: 10 QinQ: 50 Multicast: 100 ADSL2+: 1000-1031 (uses the VLAN authentication) SHDSL: 1300-1315 (uses the VLAN authentication) GPON: 1510 (the ONT uses the SN + password authentication) POTS: 1600 (uses the H.248 protocol)	NMS: 10 Stacking: 60-62 (inner label: 111-113) Triple play: 100-102 ADSL2+: 1000 (uses the PPPoE authentication) SHDSL: 1300 (uses the PPPoE authentication) POTS: 1600 (uses the H.248 protocol)	NMS: 10 Multicast: 100 ADSL2+: 1000 (uses the PPPoE authentication) SHDSL: 1300 (uses the PPPoE authentication) GPON: 1530 (the ONT uses the SN + password authentication) POTS: 1600 (uses the H.248 protocol)	NMS: 10 QinQ: 50 VDSL2: 1800 (uses the PPPoE authentication)
Slot and port	ADSL2+: 0/2 SHDSL: 0/5 GPON: 0/18 POTS: 0/3 QinQ: 0/5/15 Multicast: 0/2/2, 0/2/3	ADSL2+: 0/2 SHDSL: 0/5 POTS: 0/3 Stacking: 0/2/0-10 (map VLAN 60, ISP1) 0/2/11-20 (map VLAN 61, ISP2) 0/2/21-30 (map VLAN 62, ISP3) Triple play: 0/2/31	ADSL2+: 0/2 SHDSL: 0/5 GPON: 0/18 POTS: 0/3	SHDSL: 0/5 VDSL: 0/2 QinQ: 0/5/15
POTS service	MGC IP address: 10.30.80.65/24 Media/Signaling IP address of the MG interface: 10.176.6.33/24 Default media gateway of the MG interface: 10.176.6.62/24 IP address of the VLAN: 10.176.6.33/24 MG interface attributes: index is 0, supported protocol is H.248, coding type is text, signaling port number is 2944, port number of the active MGC is 2944, and transmission mode is UDP.			
NMS host	2.2.2.2 and 2.2.2.3			
Log host	3.3.3.3 and 3.3.4.3			
Time server	4.4.4.4 and 4.4.4.5			

Copyright © Huawei Technologies Co., Ltd.

Item	MA5600T-1	MA5600T-2	MA5600T-3	MA5600T-4
Multicast server	10.10.10.10			
EMU	Fan monitoring			
DHCP server	DHCP server1: 10.1.1.2 (active), 10.1.1.3 (standby) Gateway: 10.1.1.1/24 DHCP server2: 10.4.4.2 (active), 10.4.4.3 (standby) Gateway: 10.4.4.1/24			
Upper-layer device	The upper-layer device supports the DHCP option82 function. The BRAS supports the PITP, Stacking, and QinQ function. The BRAS supports inner and outer VLAN tags. The VLAN ID of the traffic flow sent from the IP network to the DSLAM is 100. The upper-layer device classifies the downstream traffic. Different services carry different 802.1p labels. The VLAN mapping to the DSLAM is configured at the upper-layer device.			

NOTE

- In this networking, MA5600T-1 can be replaced with a GE switch or a BRAS.
- The upstream port of the MA5600T supports the port aggregation function. In the actual network planning, you can aggregate multiple upstream ports for use.
- In this networking, the four MA5600Ts support the ADSL2+, SHDSL, VDSL2, GPON, and POTS services. You can plan the services according to your actual network conditions.

7.3 Configuring MA5600T-1

This topic describes how to configure MA5600T-1.

Procedure

Step 1 Confirm the board.

```
huawei>enable
huawei#config
huawei(config)#board confirm 0
```

Step 2 Configure the NMS.

1. Configure the IP address of the inband NMS interface.
   - Create the NMS VLAN.
     ```
     huawei(config)#vlan 10 standard
     ```
   - Add the upstream port.
     ```
     huawei(config)#port vlan 10 0/19 0-1
       It will take several minutes, and console may be timeout, please use
     command
     idle-timeout to set time
     ```


Copyright © Huawei Technologies Co., Ltd.

```
limit
  Are you sure to add standard port(s)? (y/n)[n]:y
```

- Enter the NMS VLAN interface mode.
  ```
  huawei(config)#interface vlanif 10
  ```
- Configure the IP address of the NMS interface.
  ```
  huawei(config-if-vlanif10)#ip address 10.10.1.2 255.255.255.0
  ```

2. Add the route.
   - Configure the route destined to the NMS (Trap destination address).
     ```
     huawei(config)#ip route-static 2.2.2.2 255.255.255.255 10.10.1.1
      preference 1
     huawei(config)#ip route-static 2.2.2.3 255.255.255.255 10.10.1.1
     preference 1
     ```
   - Configure the route destined to the time server.
     ```
     huawei(config)#ip route-static 4.4.4.4 255.255.255.255 10.10.1.1
     preference 1
     huawei(config)#ip route-static 4.4.4.5 255.255.255.255 10.10.1.1
     preference 1
     ```
   - Configure the route destined to the log host.
     ```
     huawei(config)#ip route-static 3.3.3.3 255.255.255.255 10.10.1.1
     preference 1
     huawei(config)#ip route-static 3.3.4.3 255.255.255.255 10.10.1.1
     preference 1
     ```
3. Add the ACL rule.
   ```
   huawei(config)#acl 3050
   huawei(config-acl-adv-3050)#rule permit ip source any destination any
   huawei(config-acl-adv-3050)#rule deny ip source any destination 10.10.1.2
    0.0.0.0
   huawei(config-acl-adv-3050)#rule permit ip source 2.2.2.2 0.0.0.0
    destination 10.10.1.2 0.0.0.0
   huawei(config-acl-adv-3050)#rule permit ip source 2.2.2.3 0.0.0.0
    destination 10.10.1.2 0.0.0.0
   huawei(config-acl-adv-3050)#rule permit ip source 4.4.4.4 0.0.0.0
    destination 10.10.1.2 0.0.0.0
   huawei(config-acl-adv-3050)#rule permit ip source 4.4.4.5 0.0.0.0
    destination 10.10.1.2 0.0.0.0
   huawei(config-acl-adv-3050)#rule permit ip source 3.3.3.3 0.0.0.0
    destination 10.10.1.2 0.0.0.0
   huawei(config-acl-adv-3050)#rule permit ip source 3.3.4.3 0.0.0.0
    destination 10.10.1.2 0.0.0.0
   huawei(config-acl-adv-3050)#quit
   huawei(config)#packet-filter inbound ip-group 3050 port 0/19/0
   huawei(config)#packet-filter inbound ip-group 3050 port 0/19/1
   ```
4. Configure SNMP.
   - Set the community name and access authority.
     ```
     huawei(config)#snmp-agent community read public
     huawei(config)#snmp-agent community write private
     ```
   - Set the SysContact.
     ```
     huawei(config)#snmp-agent sys-info contact HW-075512345678
     ```
   - Set the SysLocation.
     ```
     huawei(config)#snmp-agent sys-info location Shenzhen China
     ```
   - Set the SNMP version.

     The SNMP version must be the same as that of the NMS. In this example, the SNMP version is set as SNMP V2C.

     ```
     huawei(config)#snmp-agent sys-info version v2c
     ```
5. Enable the trap sending.

Copyright © Huawei Technologies Co., Ltd.

```
huawei(config)#snmp-agent trap enable standard
```

6. Set trap destination address.

```
huawei(config)#snmp-agent target-host trap-hostname huawei address 2.2.2.2
trap-paramsname abc
huawei(config)#snmp-agent target-host trap-hostname huawei123 address 2.2.2.3
trap-paramsname 123
```

7. Set trap source address.

```
huawei(config)#snmp-agent trap source vlanif 10
```

Step 3 Configure the time server.

```
huawei(config)#ntp-service unicast-server 4.4.4.4 source-interface vlanif 10
huawei(config)#ntp-service unicast-server 4.4.4.5 source-interface vlanif 10
```

Step 4 Configure the log host.

```
huawei(config)#loghost add 3.3.3.3 syslog-1
huawei(config)#loghost activate ip 3.3.3.3
huawei(config)#loghost add 3.3.4.3 syslog-2
huawei(config)#loghost activate ip 3.3.4.3
```

Step 5 Configure the EMU.

This topic uses the fan monitoring as an example to show how to configure the EMU.

In this example, assume that the slave node number is 1. In this case, you need to set the DIP switch of the node address on the fan monitoring unit as 1.

```
huawei(config)#emu add 0 h801ESC 0 0
huawei(config)#emu add 1 fan 0 1
```

Step 6 Configure GIU subtending.

MA5600T-1 is subtended with MA5600T-2 andMA5600T-3. Therefore, the subtending should be configured.

```
huawei(config)#vlan 60 to 62 standard
huawei(config)#port vlan 60 to 62 0/19 0-1
  It will take several minutes, and console may be timeout, please use command
idle-timeout to set time limit
  Are you sure to add standard port(s)? (y/n)[n]:y
huawei(config)#vlan 101 to 102 standard
huawei(config)#port vlan 101 to 102 0/19 0-1
  It will take several minutes, and console may be timeout, please use command
idle-timeout to set time limit
  Are you sure to add standard port(s)? (y/n)[n]:y
```

Step 7 Configure the ADSL2+ service.

The MA5600T supports the ADSL2+ service of multiple encapsulation modes, such as IPoA, PPPoA, IPoE, and PPPoE. This topic uses the PPPoE mode as an example to describe how to configure the ADSL2+ service. For other encapsulation modes, see "**3.1 Example: Configuring the xDSL Internet Access Service**."

1. Configure the ADSL2+ line profile.

   You can configure it based on your requirements.

```
huawei(config)#adsl line-profile add 10
  Start adding profile
  Press 'Q' to quit the current configuration and new configuration will be
neglected
>  Do you want to name the profile (y/n) [n]:
>    Transmission mode:
>      0: Custom
>      1: All (G992.1~5,T1.413,ETSI)
>      2: Full rate(G992.1/3/5,T1.413,ETSI)
>      3: G.DMT (G992.1/3/5)
```


Copyright © Huawei Technologies Co., Ltd.

```
>      4: G.HS (G992.1~5)
>      5: ADSL (G992.1~2,ETSI,T1.413)
>      6: ADSL2 & ADSL2+ (G992.3~5)
>    Please select (0~6) [1]:
>  Trellis mode 1-disable 2-enable (1~2) [2]:
>  Bit swap downstream 1-disable 2-enable (1~2) [2]:
>  Bit swap upstream 1-disable 2-enable (1~2) [2]:
>  Please select the form of transmit rate adaptation downstream:
>  1-fixed, 2-adaptAtStartup, 3-adaptAtRuntime (1~3) [2]:
>  Please select the form of transmit rate adaptation upstream:
>  1-fixed, 2-adaptAtStartup, 3-adaptAtRuntime (1~3) [2]:
>  Will you set SNR margin parameters? (y/n) [n]:
>  Will you set DPBO parameters? (y/n)[n]:
>  Will you set power management parameters? (y/n) [n]:
>  Will you set tone blackout configuration parameter? (y/n) [n]:
>  Will you set mode-specific parameters? (y/n) [n]:
  Add profile 10 successfully
```

2. Configure the ADSL2+ channel profile.

   The ADSL2+ channel profile should be configured based on the actual channel condition.

```
huawei(config)#adsl channel-profile add 10
  Start adding profile
  Press 'Q' to quit the current configuration and new configuration will be
neglected
>  Do you want to name the profile (y/n) [n]:
>  Will you set the minimum impulse noise protection? (y/n) [n]:y
>    Minimum impulse noise protection downstream:
>    1-noProtection    2-halfSymbol      3-singleSymbol     4-twoSymbols
>    5-threeSymbols    6-fourSymbols     7-fiveSymbols      8-sixSymbols
>    9-sevenSymbols    10-eightSymbols   11-nineSymbols     12-tenSymbols
>    13-elevenSymbols  14-twelveSymbols  15-thirteenSymbols 16-fourteenSymbols
>    17-fifteenSymbols 18-sixteenSymbols
>    Please select (1~18) [2]:4
>    Minimum impulse noise protection upstream:
>    1-noProtection    2-halfSymbol      3-singleSymbol     4-twoSymbols
>    5-threeSymbols    6-fourSymbols     7-fiveSymbols      8-sixSymbols
>    9-sevenSymbols    10-eightSymbols   11-nineSymbols     12-tenSymbols
>    13-elevenSymbols  14-twelveSymbols  15-thirteenSymbols 16-fourteenSymbols
>    17-fifteenSymbols 18-sixteenSymbols
>    Please select (1~18) [2]:4
>  Will you set interleaving delay parameters? (y/n) [n]:y
>    Maximum interleaving delay downstream (0~63 ms) [16]:24
>    Maximum interleaving delay upstream (0~63 ms) [6]:12
>  Will you set parameters for rate? (y/n) [n]:y
>    Minimum transmit rate downstream (32~32000 Kbps) [32]:
>    Minimum reserved transmit rate downstream (32~32000 Kbps) [32]:
>    Maximum transmit rate downstream (32~32000 Kbps) [24544]:8000
>    Minimum transmit rate upstream (32~6000 Kbps) [32]:
>    Minimum reserved transmit rate upstream (32~6000 Kbps) [32]:
>    Maximum transmit rate upstream (32~6000 Kbps) [1024]:
>  Will you set rate thresholds? (y/n) [n]:
  Add profile 10 successfully
```

3. Configure the ADSL2+ line template.

   Bind the configured line profile to the configured channel profile. The index of the line template is 10.

```
huawei(config)#adsl line-template add
10
  Start adding
template
  Press 'Q' to quit the current configuration and new configuration will
be
neglected
>  Do you want to name the template (y/n)
[n]:
>  Please set the line-profile index (1~128) [1]:
```


Copyright © Huawei Technologies Co., Ltd.

```
10
>  Will you set channel configuration parameters? (y/n)
[n]:y
>    Please set the channel number (1~2) [1]:
1
>    Channel1 configuration
parameters:
>    Please set the channel-profile index (1~128) [1]:
10
  Add template 10
successfully
```

4. Configure the ADSL2+ alarm profile.

   The ADSL2+ alarm profile should be configured based on the actual line condition. see "Configuring an ADSL2+ Alarm Template" for the configuration. The following uses the alarm profile 1 as an example.

5. Configure the ADSL2+ traffic profile.

   To configure the ADSL2+ traffic profile, run the **traffic table ip** command.

   In this example, the default profile (profile 6) is used.

6. Activate the ADSL2+ port.

```
huawei(config)#interface adsl 0/2
huawei(config-if-adsl-0/2)#deactivate all
huawei(config-if-adsl-0/2)#alarm-config all 1
huawei(config-if-adsl-0/2)#activate all template-index 1
huawei(config-if-adsl-0/2)#quit
```

7. Configure the upstream port.

   - Configure the GIU board.

     By default, the GE optical port of the GIU board works in the full duplex mode with the rate of 1000 Mbit/s.

     To change the port working mode and the port rate, run the **speed** and **duplex** command in the GIU mode.

     The settings must be the same as the settings of the peer device.

   - Configure the VLAN.

     The ADSL2+ users of MA5600T-1 use the VLAN authentication. In this case, the MUX VLAN is used to identify the users.

```
huawei(config)#vlan 1000 to 1031 mux
huawei(config)#port vlan 1000 0/19 0-1
  It will take several minutes, and console may be timeout, please use
command
idle-timeout to set time
limit
  Are you sure to add standard port(s)? (y/n)[n]:y
huawei(config)#port vlan 1001 to 1031 0/19 0
```

8. Add the service port.

   All ports in slot 0/3 provide the ADSL2+ service. To add service ports in batches, run the **multi-service-port** command.

```
huawei(config)#multi-service-port from-vlan 1000 port 0/2 0-31 vpi 0 vci 35
rx-cttr 6 tx-cttr 6
```

Step 8 Configure the SHDSL service.

The MA5600T supports the SHDSL service of multiple encapsulation modes, such as IPoA, PPPoA, IPoE, and PPPoE. This topic uses the PPPoE mode as an example to describe how to

Copyright © Huawei Technologies Co., Ltd.

configure the SHDSL service. For other encapsulation modes, see "**3.1 Example: Configuring the xDSL Internet Access Service**."

1. Configure the SHDSL line profile.

   To configure the SHDSL line profile, run the **shdsl line-profile add** or **shdsl line-profile quickadd** command.

```
huawei(config)#shdsl line-profile quickadd 10 line two-wire rate 2048 2048
psd
symmetric transmission Annex-A remote disable probe disable snr-margin ds-curr
10 ds-worst
 10 us-curr 10 us-worst 10 bitmap 0x03
```

2. Configure the SHDSL alarm profile.

   To configure the SHDSL alarm profile, run the **shdsl alarm-profile add** command.

   In this example, the default profile (profile 1) is used.

3. Configure the SHDSL traffic profile.

   To configure the SHDSL traffic profile, run the **traffic table ip** command.

   In this example, the default profile (profile 6) is used.

4. Activate the SHDSL port.

```
huawei(config)#interface shl 0/5
huawei(config-if-shdsl-0/5)#deactivate all
huawei(config-if-shdsl-0/5)#alarm-config all 1
huawei(config-if-shdsl-0/5)#activate all 10
huawei(config-if-shdsl-0/5)#quit
```

5. Configure the upstream port.

   The SHDSL users of MA5600T-1 use the VLAN authentication. In this case, the MUX VLAN is used to identify the users.

```
huawei(config)#vlan 1300 to 1314 mux
huawei(config)#port vlan 1300 0/19 0-1
  It will take several minutes, and console may be timeout, please use
command
idle-timeout to set time
limit
  Are you sure to add standard port(s)? (y/n)[n]:y
huawei(config)#port vlan 1300 to 1314 0/19 0
```

6. Add the service port.

   - Ports 0-15 in slot 0/5 provide the SHDSL service.
   - To add service ports in batches, run the **multi-service-port** command.

```
huawei(config)#multi-service-port from-vlan 1300 port 0/5 0-14 vpi 0 vci 35
rx-cttr 6 tx-cttr 6
```

Step 9 Configure the GPON service.

1. Configure the service VLAN and the upstream port.

```
huawei(config)#vlan 1510 smart
huawei(config)#port vlan 1510 0/19 0
```

2. Configure the DBA profile.

```
huawei(config)#tcont-profile add profile-id 10 type1 fix 102400
```

3. Configure the alarm threshold profile.

   - When you need to configure the alarm threshold value to monitor the performance statistics of the activated ONT line, run the **gpon alarm-profile add** command to configure the GPON alarm threshold profile.

Copyright © Huawei Technologies Co., Ltd.

- In the default GPON alarm threshold profile 1, all alarm thresholds are set to 0, which indicates that no alarm is reported.
- In this example, the default alarm threshold profile is used. You do not need to configure it.

4. Configure the GPON traffic profile.

```
huawei(config)#traffic table ip index 8 cir 10240 priority 0 priority-policy
tag-In-Package
```

5. Add an ONT.

NOTE

- You can add an ONT in two ways: run the **ont add** command to add an ONT offline or run the **ont confirm** command to confirm an ONT that is in the auto-find state.
- You need to run the **port ont-auto-find** command in the GPON mode to enable the auto-find function of the ONT.

```
huawei(config)#interface gpon 0/18
huawei(config-if-gpon-0/18)#ont add 1 0 hwhw-10101010 password-auth huawei
profile-id 2
```

6. Bind the alarm threshold profile.

```
huawei(config-if-gpon-0/18)#ont alarm-profile 1 0 profile-id 1
```

7. Bind the DBA profile.

```
huawei(config-if-gpon-0/18)#tcont bind-profile 1 0 1 profile-id 10
```

8. Divide the ONT port VLAN.

```
huawei(config-if-gpon-0/18)#ont port vlan 1 0 eth 10 0
huawei(config-if-gpon-0/18)#ont port native-vlan 1 0 eth 0 vlan 1510
```

9. Configure the GEM port.

```
huawei(config-if-gpon-0/18)#gemport add 1 gemportid 150 eth
```

10. Bind the GEM port to an ONT T-CONT.

NOTE

In the actual application, if the ONT terminal does not support the priority queue scheduling, you can use the CAR to limit the rate when binding the GEM port to the ONT T-CONT.

```
huawei(config-if-gpon-0/18)#ont gemport bind 1 0 150 1 priority-queue 3
```

11. Create the mapping between the GEM port and the service stream.

```
huawei(config-if-gpon-0/18)#ont gemport mapping 1 0 150 vlan 1510
huawei(config-if-gpon-0/18)#quit
```

12. Add the service port.

```
huawei(config)#service-port vlan 1510 gpon 0/18/0 gemport 150 multi-service
user-vlan 10 rx-cttr 5 tx-cttr 8
```

Step 10 Configure the POTS service.

1. Configure the upstream ports of the media stream and the signaling flow.

```
huawei(config)#vlan 1600 smart
huawei(config)#interface vlanif 1600
huawei(config)#port vlan 1600 0/19 0
huawei(config-if-vlanif1600)#ip address 10.176.6.33 24
```

2. Configure the static route destined to the MGC.

NOTE

When the MGC and the MG are in the same network segment, you do not need to configure the static route.

```
huawei(config)#ip route-static 10.30.80.0 255.255.255.0 10.176.6.62
```


Copyright © Huawei Technologies Co., Ltd.

3. Configure the media IP address pool and the signaling IP address pool.

```
huawei(config)#voip
huawei(config-voip)#ip address media 10.176.6.33 10.176.6.62
huawei(config-voip)#ip address signaling 10.176.6.33
```

4. Configure the MG interface.

   Add an MG interface.

```
huawei(config)#interface h248 0
  Are you sure to add MG interface? (y/n)[n]:y
```

   Configure the MG interface attributes.

```
huawei(config-if-h248-0)#if-h248 attribute mgip 10.176.6.33 mgport 2944 code
text
transfer udp primary-mgc-ip1 10.30.80.65 primary-mgc-port 2944 mg-media-ip1
10.176.6.33
```

   Configure the software parameters of the MG interface (in this example, only parameter 20 is configured, and other parameters use the default values).

```
huawei(config-if-h248-0)#mg-software parameter 20 2
```

5. Reset the MG interface.

   NOTE

   After configuring the MG interface, you need to reset the interface to validate the configuration.

```
huawei(config-if-h248-0)#reset coldstart
  Are you sure to reset MG interface?(y/n)[n]:y
```

6. Add PSTN users in batches.

```
huawei(config)#esl user
huawei(config-esl-user)#mgpstnuser batadd 0/3/0 0/3/31 0 terminalid 0 telno
88660032
```

Step 11 Configuring the QinQ private line service.

MA5600T-1 and MA5600T-4 serve two branches of a company to provide the QinQ private line service.

1. Create VLAN 50.

```
huawei(config)#vlan 50 mux
```

2. Set VLAN 50 as QinQ VLAN.

```
huawei(config)#vlan attrib 50 q-in-q
```

3. Add the upstream port.

```
huawei(config)#port vlan 50 0/19 0
```

4. Add the service port.

   To add the service port, run the **service-port** command. Note that the VPI and VCI values of the virtual port must be the same as those on the modem.

   The QinQ VLAN supports the PVC-priority scheduling policy only. In this case, select the profile that supports PVC-priority policy.

```
huawei(config)#traffic table ip index 7 cir off priority 0 priority-policy
local-Setting
huawei(config)#service-port vlan 50 shdsl 0/5/15 vpi 0 vci 35 rx-cttr 7
tx-cttr 7
```

Step 12 Configure the multicast service.

After the configuration, the following results should be achieved:

Copyright © Huawei Technologies Co., Ltd.

- Users of port 0/2/2 need to be authenticated, and have rights to watch two programs and to preview one program.
- Users of port 0/2/3 do not need to be authenticated.

1. Configure the xDSL.

   In this example, there is no need to configure the xDSL. The default line profile (profile 1002) is used.

2. Configure the VLAN.

   - Create a VLAN.
     ```
     huawei(config)#vlan 100 smart
     ```
   - Configure the VLAN upstream port.
     ```
     huawei(config)#port vlan 100 0/19 0-1
       It will take several minutes, and console may be timeout, please use
     command
     idle-timeout to set time
     limit
       Are you sure to add standard port(s)? (y/n)[n]:y
     ```
   - Configure the native VLAN.

     NOTE

     When the VLAN ID of the tag packet is the same as the VLAN ID of the native VLAN of the egress, the egress removes the tag of the packet. That is, the tagged packet becomes to the untagged packet (without VLAN ID) after the tagged packet passes through the egress.

     ```
     huawei(config)#interface giu 0/19
     huawei(config-if-giu-0/19)#native-vlan 0 vlan 100
     huawei(config-if-giu-0/19)#native-vlan 1 vlan 100
     ```
   - Create the traffic profile.
     ```
     huawei(config)#traffic table ip index 8 cir off priority 5 priority-policy
     local-Setting
     ```
   - Add ADSL2+ ports 0/0/2 and 0/0/3 to VLAN 100.
     ```
     huawei(config)#service-port vlan 100 adsl 0/2/2 vpi 0 vci 35 rx-cttr 8 tx-
     cttr 8
     huawei(config)#service-port vlan 100 adsl 0/2/3 vpi 0 vci 35 rx-cttr 8 tx-
     cttr 8
     ```

3. Configure the multicast service.

   - Enable the multicast proxy function.
     ```
     huawei(config)#multicast-vlan 100
     huawei(config-mvlan100)#igmp mode proxy
       Are you sure to change IGMP mode?(y/n)[n]:y
     ```
   - Set the upstream port.
     ```
     huawei(config-mvlan100)#igmp uplink-port 0/19/0
     huawei(config-mvlan100)#quit
     huawei(config)#btv
     huawei(config-btv)#igmp uplink-port-mode default
     Are you sure to change the uplink port mode?(y/n)[n]:y
     ```
   - Set the preview parameters.

     In this example, configure the preview authority profile with the preview duration for the program to 150s, the number of preview attempts to 6 each day and the preview interval to 60s.

     ```
     huawei(config-btv)#igmp preview-profile add index 1 duration 150 times 6
     interval 60
     huawei(config-btv)#igmp preview auto-reset-time 00:00:00
     huawei(config-btv)#quit
     ```


Copyright © Huawei Technologies Co., Ltd.

- Configured the program library.
```
huawei(config)#multicast-vlan 100
huawei(config-mvlan100)#igmp program add name program1 ip 224.1.1.1 sourceip 10.10.10.10
huawei(config-mvlan100)#igmp program add name program2 ip 224.1.1.2 sourceip 10.10.10.10
huawei(config-mvlan100)#igmp program add name program3 ip 224.1.1.3 sourceip 10.10.10.10 preview-profile 1
huawei(config-mvlan100)#quit
```
- Configure the authority profile.
```
huawei(config)#btv
huawei(config-btv)#igmp profile add profile-name profile0
huawei(config-btv)#igmp profile profile-name profile0 program-name program1 watch
huawei(config-btv)#igmp profile profile-name profile0 program-name program2 watch
huawei(config-btv)#igmp profile profile-name profile0 program-name program3 preview
```
- Configure the multicast user.
```
huawei(config-btv)#igmp user add port 0/2/3 adsl 0 35 no-auth
huawei(config-btv)#igmp user add port 0/2/2 adsl 0 35 auth
huawei(config-btv)#igmp user bind-profile port 0/2/2 profile-name profile0
huawei(config-btv)#quit
huawei(config)#multicast-vlan 100
huawei(config-mvlan100)#igmp multicast-vlan member port 0/2/2
huawei(config-mvlan100)#igmp multicast-vlan member port 0/2/3
```

Step 13 Configure the subtending multicast service.

1. Set the upstream port.

   The upstream port is already configured in **Step 12.3**.
2. Configure the IGMP proxy.

   The IGMP proxy is already configured in **Step 12.3**.
3. Configure the program library.

   The program library is already configured in **Step 12.3**.
4. Configure the multicast for the subtending port.
   - Specify a subtending port.
```
huawei(config-btv)#igmp cascade-port 0/19/1
```
   - Modify a subtending port.
```
huawei(config-btv)#igmp cascade-port modify 0/19/1 static enable
```
   - Add programs for the static subtending port.
```
huawei(config-btv)#igmp static-join cascade-port 0/19/1 ip 224.1.1.1 vlan 100
huawei(config-btv)#igmp static-join cascade-port 0/19/1 ip 224.1.1.2 vlan 100
huawei(config-btv)#igmp static-join cascade-port 0/19/1 ip 224.1.1.3 vlan 100
huawei(config-btv)#quit
```

Step 14 Save the data.
```
huawei(config)#save
```

----End

7.4 Configuring MA5600T-2

This topic describes how to configure MA5600T-2.

Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Confirm the board.

```
huawei>enable
huawei#config
huawei(config)#board confirm 0
```

Step 2 Configure the NMS.

1. Configure the IP address of the inband NMS interface.
   - Create the NMS VLAN.
     ```
     huawei(config)#vlan 10 standard
     ```
   - Add the upstream port.
     ```
     huawei(config)#port vlan 10 0/19 0-1
       It will take several minutes, and console may be timeout, please use
     command
     idle-timeout to set time
     limit
       Are you sure to add standard port(s)? (y/n)[n]:y
     ```
   - Enter the NMS VLAN interface mode.
     ```
     huawei(config)#interface vlanif 10
     ```
   - Configure the IP address of the NMS interface.
     ```
     huawei(config-if-vlanif10)#ip address 10.10.1.3 255.255.255.0
     ```
2. Add the route.
   - Configure the route destined to the NMS (Trap destination address).
     ```
     huawei(config)#ip route-static 2.2.2.2 255.255.255.255 10.10.1.1
     preference 1
     huawei(config)#ip route-static 2.2.2.3 255.255.255.255 10.10.1.1
     preference 1
     ```
   - Configure the route destined to the time server.
     ```
     huawei(config)#ip route-static 4.4.4.4 255.255.255.255 10.10.1.1
     preference 1
     huawei(config)#ip route-static 4.4.4.5 255.255.255.255 10.10.1.1
     preference 1
     ```
   - Configure the route destined to the log host.
     ```
     huawei(config)#ip route-static 3.3.3.3 255.255.255.255 10.10.1.1
     preference 1
     huawei(config)#ip route-static 3.3.4.3 255.255.255.255 10.10.1.1
     preference 1
     ```
3. Add the ACL rule.

```
huawei(config)#acl 3050
huawei(config-acl-adv-3050)#rule permit ip source any destination any
huawei(config-acl-adv-3050)#rule deny ip source any destination 10.10.1.2
0.0.0.0
huawei(config-acl-adv-3050)#rule permit ip source 2.2.2.2 0.0.0.0
destination 10.10.1.2 0.0.0.0
huawei(config-acl-adv-3050)#rule permit ip source 2.2.2.3 0.0.0.0
destination 10.10.1.2 0.0.0.0
huawei(config-acl-adv-3050)#rule permit ip source 4.4.4.4 0.0.0.0
destination 10.10.1.2 0.0.0.0
huawei(config-acl-adv-3050)#rule permit ip source 4.4.4.5 0.0.0.0
destination 10.10.1.2 0.0.0.0
huawei(config-acl-adv-3050)#rule permit ip source 3.3.3.3 0.0.0.0
destination 10.10.1.2 0.0.0.0
huawei(config-acl-adv-3050)#rule permit ip source 3.3.4.3 0.0.0.0
destination 10.10.1.2 0.0.0.0
huawei(config-acl-adv-3050)#quit
huawei(config)#packet-filter inbound ip-group 3050 port 0/19/0
huawei(config)#packet-filter inbound ip-group 3050 port 0/19/1
```


Copyright © Huawei Technologies Co., Ltd.

4. Configure SNMP.
   - Set the community name and access authority.
     ```
     huawei(config)#snmp-agent community read public
     huawei(config)#snmp-agent community write private
     ```
   - Set the SysContact.
     ```
     huawei(config)#snmp-agent sys-info contact HW-075512345678
     ```
   - Set the SysLocation.
     ```
     huawei(config)#snmp-agent sys-info location Shenzhen China
     ```
   - Set the SNMP version.

     The SNMP version must be the same as the SNMP version of the NMS. In this example, the SNMP version is set as SNMP V2C.

     ```
     huawei(config)#snmp-agent sys-info version v2c
     ```
5. Enable the trap sending.
   ```
   huawei(config)#snmp-agent trap enable standard
   ```
6. Set trap destination address.
   ```
   huawei(config)#snmp-agent target-host trap-hostname huawei address 2.2.2.2
   trap-paramsname abc
   huawei(config)#snmp-agent target-host trap-hostname huawei123 address 2.2.2.3
   trap-paramsname 123
   ```
7. Set the trap source address.
   ```
   huawei(config)#snmp-agent trap source vlanif 10
   ```

Step 3 Configure the time server.

```
huawei(config)#ntp-service unicast-server 4.4.4.4 source-interface vlanif 10
huawei(config)#ntp-service unicast-server 4.4.4.5 source-interface vlanif 10
```

Step 4 Configure the log host.

```
huawei(config)#loghost add 3.3.3.3 syslog-1
huawei(config)#loghost activate ip 3.3.3.3
huawei(config)#loghost add 3.3.4.3 syslog-2
huawei(config)#loghost activate ip 3.3.4.3
```

Step 5 Configure the EMU.

This topic uses the fan monitoring as an example to show how to configure the EMU.

By default, the default slave node number of the fan EMU is 0. In this example, assume that the slave node number 1. In this case, you need to set the DIP switch of the node address on the fan monitoring unit as 1.

```
huawei(config)#emu add 0 h801esc 0 0
huawei(config)#emu add 1 fan 0 1
```

Step 6 Configure GIU subtending

MA5600T-2 is subtended with MA5600T-3. Therefore subtending should be configured transparently transmit the VLAN data of MA5600T-3. There are four VLANs configured on MA5600T-3, with the VLAN ID of 10, 100, 1000 and 1300.

These VLAN are already configured with subtending, and it is unnecessary to configure them again.

Step 7 Configure the ADSL2+ service.

The MA5600T supports the ADSL2+ service of multiple encapsulation modes, such as IPoA, PPPoA, IPoE, and PPPoE. This topic uses the PPPoE mode as an example to describe how to configure the ADSL2+ service. For other encapsulation modes, see "**3.1 Example: Configuring the xDSL Internet Access Service**."

Copyright © Huawei Technologies Co., Ltd.

1. Configure the ADSL2+ line profile.

   You can configure it based on your requirements.

```
huawei(config)#adsl line-profile add 10
  Start adding profile
  Press 'Q' to quit the current configuration and new configuration will be
neglected
>  Do you want to name the profile (y/n) [n]:
>    Transmission mode:
>      0: Custom
>      1: All (G992.1~5,T1.413,ETSI)
>      2: Full rate(G992.1/3/5,T1.413,ETSI)
>      3: G.DMT (G992.1/3/5)
>      4: G.HS (G992.1~5)
>      5: ADSL (G992.1~2,ETSI,T1.413)
>      6: ADSL2 & ADSL2+ (G992.3~5)
>    Please select (0~6) [1]:
>  Trellis mode 1-disable 2-enable (1~2) [2]:
>  Bit swap downstream 1-disable 2-enable (1~2) [2]:
>  Bit swap upstream 1-disable 2-enable (1~2) [2]:
>  Please select the form of transmit rate adaptation downstream:
>  1-fixed, 2-adaptAtStartup, 3-adaptAtRuntime (1~3) [2]:
>  Please select the form of transmit rate adaptation upstream:
>  1-fixed, 2-adaptAtStartup, 3-adaptAtRuntime (1~3) [2]:
>  Will you set SNR margin parameters? (y/n) [n]:
>  Will you set DPBO parameters? (y/n)[n]:
>  Will you set power management parameters? (y/n) [n]:
>  Will you set tone blackout configuration parameter? (y/n) [n]:
>  Will you set mode-specific parameters? (y/n) [n]:
  Add profile 10 successfully
```

2. Configure the ADSL2+ channel profile.

   The configuration data in the ADSL2+ channel profile is set according to the actual channel conditions.

```
huawei(config)#adsl channel-profile add 10
  Start adding profile
  Press 'Q' to quit the current configuration and new configuration will be
neglected
>  Do you want to name the profile (y/n) [n]:
>  Will you set the minimum impulse noise protection? (y/n) [n]:y
>    Minimum impulse noise protection downstream:
>    1-noProtection    2-halfSymbol      3-singleSymbol     4-twoSymbols
>    5-threeSymbols    6-fourSymbols     7-fiveSymbols      8-sixSymbols
>    9-sevenSymbols    10-eightSymbols   11-nineSymbols     12-tenSymbols
>    13-elevenSymbols  14-twelveSymbols  15-thirteenSymbols 16-fourteenSymbols
>    17-fifteenSymbols 18-sixteenSymbols
>    Please select (1~18) [2]:4
>    Minimum impulse noise protection upstream:
>    1-noProtection    2-halfSymbol      3-singleSymbol     4-twoSymbols
>    5-threeSymbols    6-fourSymbols     7-fiveSymbols      8-sixSymbols
>    9-sevenSymbols    10-eightSymbols   11-nineSymbols     12-tenSymbols
>    13-elevenSymbols  14-twelveSymbols  15-thirteenSymbols 16-fourteenSymbols
>    17-fifteenSymbols 18-sixteenSymbols
>    Please select (1~18) [2]:4
>  Will you set interleaving delay parameters? (y/n) [n]:y
>    Maximum interleaving delay downstream (0~63 ms) [16]:24
>    Maximum interleaving delay upstream (0~63 ms) [6]:12
>  Will you set parameters for rate? (y/n) [n]:y
>    Minimum transmit rate downstream (32~32000 Kbps) [32]:
>    Minimum reserved transmit rate downstream (32~32000 Kbps) [32]:
>    Maximum transmit rate downstream (32~32000 Kbps) [24544]:8000
>    Minimum transmit rate upstream (32~6000 Kbps) [32]:
>    Minimum reserved transmit rate upstream (32~6000 Kbps) [32]:
>    Maximum transmit rate upstream (32~6000 Kbps) [1024]:
>  Will you set rate thresholds? (y/n) [n]:
  Add profile 10 successfully
```


Copyright © Huawei Technologies Co., Ltd.

3. Configure the ADSL2+ line template.

   Bind the configured line profile and channel profile together to form line template 10.

```
huawei(config)#adsl line-template add 10
  Start adding template
  Press 'Q' to quit the current configuration and new configuration will be
neglected
>  Do you want to name the template (y/n) [n]:
>  Please set the line-profile index (1~128) [1]:10
>  Will you set channel configuration parameters? (y/n) [n]:y
>    Please set the channel number (1~2) [1]:1
>    Channel1 configuration parameters:
>    Please set the channel-profile index (1~128) [1]:10
Add template 10 successfully
```

4. Configure the ADSL2+ alarm profile.

   You can configure the ADSL2+ alarm profile based on your own needs. For details, see "Configuring an ADSL2+ Alarm Template." In this example, the default alarm profile (template 1) is used.

5. Configure the ADSL2+ traffic profile.

   To configure the ADSL2+ traffic profile, run the **traffic table ip** command.

   In this example, the default profile (profile 6) is used.

6. Activate the ADSL2+ port.

```
huawei(config)#interface adsl 0/2
huawei(config-if-adsl-0/2)#deactivate all
huawei(config-if-adsl-0/2)#alarm-config all 1
huawei(config-if-adsl-0/2)#activate all 10
huawei(config-if-adsl-0/2)#quit
```

7. Configure the upstream port.

   - Configure the GIU board.

     By default, the GE optical port of the GIU board works in the full duplex mode with the rate of 1000 Mbit/s.

     To change the port working mode and the port rate, run the **speed** and **duplex** commands in GIU mode.

     The settings must be the same as the settings of the peer device.

   - Configure the VLAN.

     The ADSL2+ users of MA5600T-1 use the VLAN authentication. In this case, the smart VLAN is used to identify the users.

```
huawei(config)#vlan 2020 smart
huawei(config)#port vlan 2020 0/19 0-1
  It will take several minutes, and console may be timeout, please use
command
idle-timeout to set time
limit
  Are you sure to add standard port(s)? (y/n)[n]:y
```

8. Add the service port.

   All ports in slot 0/2 provide the ADSL2+ service. To add service ports in batches, run the **multi-service-port** command.

```
huawei(config)#multi-service-port vlan 2020 port 0/2 0-31 vpi 0 vci 35 user-
encap pppo
 rx-cttr 6 tx-cttr 6
```

Step 8 Configure the SHDSL service.

Copyright © Huawei Technologies Co., Ltd.

The MA5600T supports the SHDSL service of multiple encapsulation modes, such as IPoA, PPPoA, IPoE, and PPPoE. This topic uses the PPPoE mode as an example to describe how to configure the SHDSL service. For other encapsulation modes, see "**3.1 Example: Configuring the xDSL Internet Access Service**."

1. Configure the SHDSL line profile.

   To configure the SHDSL line profile, run the **shdsl line-profile add** or **shdsl line-profile quickadd** command.

   ```
   huawei(config)#shdsl line-profile quickadd 10 line two-wire rate 2048 2048
   psd
   symmetric transmission Annex-A remote disable probe disable snr-margin ds-curr
   10 ds-worst
    10 us-curr 10 us-worst 10 bitmap 0x03
   ```

2. Configure the SHDSL alarm profile.

   To configure the SHDSL alarm profile, run the **shdsl alarm-profile add** command.

   In this example, the default profile (profile 1) is used.

3. Configure the SHDSL traffic profile.

   To configure the SHDSL traffic profile, run the **traffic table ip** command.

   In this example, the default profile (profile 6) is used.

4. Activate the SHDSL port.

   ```
   huawei(config)#interface shl 0/5
   huawei(config-if-shdsl-0/5)#deactivate all
   huawei(config-if-shdsl-0/5)#alarm-config all 1
   huawei(config-if-shdsl-0/5)#activate all 10
   huawei(config-if-shdsl-0/5)#quit
   ```

5. Configure the upstream port.

   The SHDSL users of MA5600T-2 use the PPPoE authentication. In this case, the smart VLAN is used to identify the users.

   ```
   huawei(config)#vlan 3020 smart
   huawei(config)#port vlan 3020 0/19 0-1
     It will take several minutes, and console may be timeout, please use
   command
   idle-timeout to set time
   limit
     Are you sure to add standard port(s)? (y/n)[n]:y
   ```

6. Add the service port.

   - Ports 0-15 of in slot 0/5 provide the SHDSL service.
   - To add service ports in batches, run the **multi-service-port** command.

   ```
   huawei(config)#multi-service-port vlan 3020 port 0/5 0-15 vpi 0 vci 35 user-
   encap
   pppoe rx-cttr 6 tx-cttr 6
   ```

Step 9 Configure the POTS service.

1. Configure the upstream ports of the media stream and the signaling flow.

   ```
   huawei(config)#vlan 1600 smart
   huawei(config)#interface vlanif 1600
   huawei(config)#port vlan 1600 0/19 0
   huawei(config-if-vlanif1600)#ip address 10.176.6.33 24
   ```

2. Configure the static route destined to the MGC.

   NOTE

   When the MGC and the MG are in the same network segment, you do not need to configure the static route.

Copyright © Huawei Technologies Co., Ltd.

```
huawei(config)#ip route-static 10.30.80.0 255.255.255.0 10.176.6.62
```

3. Configure the media IP address pool and the signaling IP address pool.

```
huawei(config)#voip
huawei(config-voip)#ip address media 10.176.6.33 10.176.6.62
huawei(config-voip)#ip address signaling 10.176.6.33
```

4. Configure the MG interface.

   Add an MG interface.

```
huawei(config)#interface h248 0
  Are you sure to add MG interface? (y/n)[n]:y
```

   Configure the MG interface attributes.

```
huawei(config-if-h248-0)#if-h248 attribute mgip 10.176.6.33 mgport 2944 code
text
 transfer udp mgcip_1 10.30.80.65 mgcport_1 2944 mg-media-ip 10.176.6.33
```

   Configure the software parameters of the MG interface (in this example, only parameter 20 is configured, and other parameters use the default values).

```
huawei(config-if-h248-0)#mg-software parameter 20 2
```

5. Reset the MG interface.

   NOTE

   After configuring the MG interface, you need to reset the interface to validate the configuration.

```
huawei(config-if-h248-0)#reset coldstart
  Are you sure to reset MG interface?(y/n)[n]:y
```

6. Add PSTN users in batches.

```
huawei(config)#esl user
huawei(config-esl-user)#mgpstnuser batadd 0/3/0 0/3/31 0 terminalid 0 telno
88660032
```

Step 10 Configure the stacking multi-ISP wholesale service.

- ISP1 provides users of ports 0/2/0 to 0/2/10 with the multi-ISP wholesale service.
- ISP2 provides users of ports 0/2/11 to 0/2/20 with the multi-ISP wholesale service.
- ISP3 provides users of ports 0/2/21 to 0/2/30 with the multi-ISP wholesale service.

1. Create a stacking VLAN.

```
huawei(config)#vlan 60 to 62 smart
huawei(config)#vlan attrib 60 to 62 stacking
huawei(config)#stacking outer-ethertype 0x8000
```

2. Add the upstream port.

```
huawei(config)#port vlan 60 to 62 0/19 0
```

3. Add the service port.

```
huawei(config)#multi-service-port vlan 60 adsl 0/2 0-10 vpi 0 vci 35
 rx-cttr 6 tx-cttr 6
huawei(config)#multi-service-port vlan 61 adsl 0/2 11-20 vpi 0 vci 35
 rx-cttr 6 tx-cttr 6
huawei(config)#multi-service-port vlan 62 adsl 0/2 21-30 vpi 0 vci 35
 rx-cttr 6 tx-cttr 6
```

4. Configure the inner label.

```
huawei(config)#stacking label vlan 60 baselabel 111
huawei(config)#stacking label vlan 61 baselabel 112
huawei(config)#stacking label vlan 62 baselabel 113
```

Step 11 Configure the triple play service.

Copyright © Huawei Technologies Co., Ltd.

After the configuration, the following results should be achieved: Uses of port 0/2/31 can watch the programs stored on servers 224.1.1.1 and 224.1.1.2, and can preview the programs stored on server 224.1.1.3.

1. Configure the upstream port and the VLAN.

```
huawei(config)#vlan 100 smart
huawei(config)#port vlan 100 0/19 0-1
  It will take several minutes, and console may be timeout, please use
command
idle-timeout to set time
limit
  Are you sure to add standard port(s)? (y/n)[n]:y
huawei(config)#vlan 101 mux
huawei(config)#port vlan 101 0/19 0
huawei(config)#vlan 102 smart
huawei(config)#port vlan 102 0/19 0
```

2. Configure the traffic table.

   The voice service has the highest priority, and the network access service has the lowest priority.

   Assume that the network access service uses traffic table 6, with the priority of 0. The following shows how to create the new traffic tables for the voice service and video service respectively.

```
huawei(config)#traffic table ip index 7 cir 1024 priority 7 priority-policy
Tag-In-Package
  Create traffic descriptor record
successfully

-------------------------------------------------
  TD Index             :
7
  TD Name              : ip-traffic-
table_7
  Priority             :
7
  Copy Priority        :
-
  Mapping Index        :
-
  CTAG Mapping Priority:
-
  CTAG Mapping Index   :
-
  CTAG Default Priority:
0
  Priority Policy      : tag-
pri
  CIR                  : 1024
kbps
  CBS                  : 34768
bytes
  PIR                  : 2048
kbps
  PBS                  : 67536
bytes
  Referenced Status    : not
used

-------------------------------------------------
huawei(config)#traffic table ip index 8 cir off priority 5 priority-policy tag-
In-Package
  Create traffic descriptor record
successfully
```


Copyright © Huawei Technologies Co., Ltd.

```
------------------------------------------------
  TD Index             :
8
  TD Name              : ip-traffic-
table_8
  Priority             :
5
  Copy Priority        :
-
  Mapping Index        :
-
  CTAG Mapping Priority:
-
  CTAG Mapping Index   :
-
  CTAG Default Priority:
0
  Priority Policy      : tag-
pri
  CIR                  :
off
  CBS                  :
off
  PIR                  :
off
  PBS                  :
off
  Referenced Status    : not
used

------------------------------------------------
```

3. Configure the service port.

```
huawei(config)#service-port vlan 100 adsl 0/2/31 vpi 0 vci 35
rx-cttr 8 tx-cttr 8
huawei(config)#service-port vlan 101 adsl 0/2/31 vpi 0 vci 36
rx-cttr 6 tx-cttr 6
huawei(config)#service-port vlan 102 adsl 0/2/31 vpi 0 vci 37
rx-cttr 7 tx-cttr 7
```

4. Configure DHCP relay mode for video service.
   - Enable DHCP mode.
     ```
     huawei(config)#dhcp mode layer-3 option-60
     ```
   - Configure the DHCP server.
     ```
     huawei(config)#dhcp-server 1 ip 10.1.1.2 10.1.1.3
     huawei(config)#dhcp domain video
     huawei(config-dhcp-domain-video)#dhcp-server 1
     ```
   - Configure the gateway mapped to the DHCP domain.
     ```
     huawei(config)#interface vlanif 100
     huawei(config-if-vlanif100)#ip address 10.1.1.1 24
     huawei(config-if-vlanif100)#dhcp domain video gateway 10.1.1.1
     ```
   - Enable DHCP Option82.
     ```
     huawei(config)#dhcp option82 enable
     ```
5. Configure DHCP relay mode for voice service.
   - Configure the DHCP server.
     ```
     huawei(config)#dhcp-server 2 ip 10.4.4.2 10.4.4.3
     huawei(config)#dhcp domain voice
     huawei(config-dhcp-domain-voice)#dhcp-server 2
     ```
   - Configure the gateway mapped to the DHCP domain.
     ```
     huawei(config)#interface vlanif 102
     huawei(config-if-vlanif102)#ip address 10.4.4.1 24
     huawei(config-if-vlanif102)#dhcp domain voice gateway 10.4.4.1
     ```


Copyright © Huawei Technologies Co., Ltd.

- Enable the DHCP option82.
  ```
  huawei(config)#dhcp option82 enable
  ```

6. Configure the multicast service.

```
huawei(config)#interface giu 0/19
huawei(config-if-giu-0/19)#native-vlan 0 vlan 100
huawei(config-if-giu-0/19)#quit
huawei(config)#multicast-vlan 100
huawei(config-mvlan100)#igmp mode proxy
  Are you sure to change IGMP mode?(y/n)[n]:y
huawei(config-mvlan100)#igmp uplink-port 0/19/0
huawei(config-mvlan100)#quit
huawei(config)#btv
huawei(config-btv)#igmp uplink-port-mode mstp
Are you sure to change the uplink port mode?(y/n)[n]:y
huawei(config-btv)#quit
huawei(config)#multicast-vlan 100
huawei(config-mvlan100)#igmp program add name program1 ip 224.1.1.1 sourceip
10.10.10.10
huawei(config-mvlan100)#igmp program add name program2 ip 224.1.1.2 sourceip
10.10.10.10
huawei(config-mvlan100)#igmp program add name program3 ip 224.1.1.3 sourceip
10.10.10.10
huawei(config-mvlan100)#quit
huawei(config)#btv
huawei(config-btv)#igmp profile add profile-name profile0
huawei(config-btv)#igmp profile profile-name profile0 program-name program1
watch
huawei(config-btv)#igmp profile profile-name profile0 program-name program2
watch
huawei(config-btv)#igmp profile profile-name profile0 program-name program3
preview
huawei(config-btv)#igmp user add port 0/2/31 auth
huawei(config-btv)#igmp user bind-profile port 0/2/31 profile-name profile0
huawei(config-btv)#quit
huawei(config)#multicast-vlan 100
huawei(config-mvlan100)#igmp multicast-vlan member port 0/2/31
```

Step 12 Configure the subtending multicast service.

1. Configure the upstream port.

   The upstream port is already configured in **Step 11.6**.

2. Configure the IGMP proxy.

   The IGMP proxy is already configured in **Step 11.6**.

3. Configure the program library.

   The program library is already configured in **Step 11.6**

4. Configure the multicast for the subtending port.

   - Specify a subtending port.
     ```
     huawei(config-btv)#igmp cascade-port 0/19/1
     ```
   - Modify a subtending port.
     ```
     huawei(config-btv)#igmp cascade-port modify 0/19/1 static enable
     ```
   - Add programs for the static subtending port.
     ```
     huawei(config-btv)#igmp static-join cascade-port 0/19/1 ip 224.1.1.1 vlan
     100
     huawei(config-btv)#igmp static-join cascade-port 0/19/1 ip 224.1.1.2 vlan
     100
     huawei(config-btv)#igmp static-join cascade-port 0/19/1 ip 224.1.1.3 vlan
     100
     huawei(config-btv)#quit
     ```


Copyright © Huawei Technologies Co., Ltd.

Step 13 Save the data.

```
huawei(config)#save
```

----End

7.5 Configuring MA5600T-3

This topic describes how to configure MA5600T-3.

Procedure

Step 1 Confirm the board.

```
huawei>enable
huawei#config
huawei(config)#board confirm 0
```

Step 2 Configure the NMS.

1. Configure the IP address of the inband NMS interface.
   - Create the NMS VLAN.
     ```
     huawei(config)#vlan 10 standard
     ```
   - Add the upstream port.
     ```
     huawei(config)#port vlan 10 0/19 0
     ```
   - Enter the NMS VLAN interface mode.
     ```
     huawei(config)#interface vlanif 10
     ```
   - Configure the IP address of the NMS interface.
     ```
     huawei(config-if-vlanif10)#ip address 10.10.1.4 255.255.255.0
     ```
2. Add the route.
   - Configure the route destined to the NMS (Trap destination address).
     ```
     huawei(config)#ip route-static 2.2.2.2 255.255.255.255 10.10.1.1
     preference 1
     huawei(config)#ip route-static 2.2.2.3 255.255.255.255 10.10.1.1
     preference 1
     ```
   - Configure the route destined to the time server.
     ```
     huawei(config)#ip route-static 4.4.4.4 255.255.255.255 10.10.1.1
     preference 1
     huawei(config)#ip route-static 4.4.4.5 255.255.255.255 10.10.1.1
     preference 1
     ```
   - Configure the route destined to the log host.
     ```
     huawei(config)#ip route-static 3.3.3.3 255.255.255.255 10.10.1.1
     preference 1
     huawei(config)#ip route-static 3.3.4.3 255.255.255.255 10.10.1.1
     preference 1
     ```
3. Add the ACL rule.

```
huawei(config)#acl 3050
huawei(config-acl-adv-3050)#rule permit ip source any destination any
huawei(config-acl-adv-3050)#rule deny ip source any destination 10.10.1.2
0.0.0.0
huawei(config-acl-adv-3050)#rule permit ip source 2.2.2.2 0.0.0.0
destination 10.10.1.2 0.0.0.0
huawei(config-acl-adv-3050)#rule permit ip source 2.2.2.3 0.0.0.0
destination 10.10.1.2 0.0.0.0
huawei(config-acl-adv-3050)#rule permit ip source 4.4.4.4 0.0.0.0
destination 10.10.1.2 0.0.0.0
huawei(config-acl-adv-3050)#rule permit ip source 4.4.4.5 0.0.0.0
destination 10.10.1.2 0.0.0.0
```


Copyright © Huawei Technologies Co., Ltd.

```
huawei(config-acl-adv-3050)#rule permit ip source 3.3.3.3 0.0.0.0
destination 10.10.1.2 0.0.0.0
huawei(config-acl-adv-3050)#rule permit ip source 3.3.4.3 0.0.0.0
destination 10.10.1.2 0.0.0.0
huawei(config-acl-adv-3050)#quit
huawei(config)#packet-filter inbound ip-group 3050 port 0/19/0
huawei(config)#packet-filter inbound ip-group 3050 port 0/19/1
```

4. Configure SNMP.
   - Set the community name and access authority.
     ```
     huawei(config)#snmp-agent community read public
     huawei(config)#snmp-agent community write private
     ```
   - Set the SysContact.
     ```
     huawei(config)#snmp-agent sys-info contact HW-075512345678
     ```
   - Set the SysLocation.
     ```
     huawei(config)#snmp-agent sys-info location Shenzhen China
     ```
   - Set the SNMP version.

     The SNMP version must be the same as the SNMP version of the NMS. In this example, the SNMP version is set as SNMP V2C.

     ```
     huawei(config)#snmp-agent sys-info version v2c
     ```
5. Enable the trap sending.
   ```
   huawei(config)#snmp-agent trap enable standard
   ```
6. Set trap destination address.
   ```
   huawei(config)#snmp-agent target-host trap-hostname huawei address 2.2.2.2
   trap-paramsname abc
   huawei(config)#snmp-agent target-host trap-hostname huawei123 address 2.2.2.3
    trap-paramsname 123
   ```
7. Set the trap source address.
   ```
   huawei(config)#snmp-agent trap source vlanif 10
   ```

Step 3 Configure the time server.

```
huawei(config)#ntp-service unicast-server 4.4.4.4 source-interface vlanif 10
huawei(config)#ntp-service unicast-server 4.4.4.5 source-interface vlanif 10
```

Step 4 Configure the log host.

```
huawei(config)#loghost add 3.3.3.3 syslog-1
huawei(config)#loghost activate ip 3.3.3.3
huawei(config)#loghost add 3.3.4.3 syslog-2
huawei(config)#loghost activate ip 3.3.4.3
```

Step 5 Configure the EMU.

This topic uses the fan monitoring as an example to show how to configure the EMU.

By default, the default slave node number of the fan EMU is 0. In this example, assume that the slave node number is 1. In this case, you need to set the DIP switch of the node address on the fan monitoring unit as 1.

```
huawei(config)#emu add 0 h801ESC 0 0
huawei(config)#emu add 1 fan 0 1
```

Step 6 Configure the ADSL2+ service.

The MA5600T supports the ADSL2+ service of multiple encapsulation modes, such as IPoA, PPPoA, IPoE, and PPPoE. This topic uses the PPPoE mode as an example to describe how to configure the ADSL2+ service. For other encapsulation modes, see "**3.1 Example: Configuring the xDSL Internet Access Service**."

Copyright © Huawei Technologies Co., Ltd.

1. Configure the ADSL2+ line profile.

   You can configure it based on your requirements.

```
huawei(config)#adsl line-profile add 10
  Start adding profile
  Press 'Q' to quit the current configuration and new configuration will be
neglected
>  Do you want to name the profile (y/n) [n]:
>    Transmission mode:
>      0: Custom
>      1: All (G992.1~5,T1.413,ETSI)
>      2: Full rate(G992.1/3/5,T1.413,ETSI)
>      3: G.DMT (G992.1/3/5)
>      4: G.HS (G992.1~5)
>      5: ADSL (G992.1~2,ETSI,T1.413)
>      6: ADSL2 & ADSL2+ (G992.3~5)
>    Please select (0~6) [1]:
>  Trellis mode 1-disable 2-enable (1~2) [2]:
>  Bit swap downstream 1-disable 2-enable (1~2) [2]:
>  Bit swap upstream 1-disable 2-enable (1~2) [2]:
>  Please select the form of transmit rate adaptation downstream:
>  1-fixed, 2-adaptAtStartup, 3-adaptAtRuntime (1~3) [2]:
>  Please select the form of transmit rate adaptation upstream:
>  1-fixed, 2-adaptAtStartup, 3-adaptAtRuntime (1~3) [2]:
>  Will you set SNR margin parameters? (y/n) [n]:
>  Will you set DPBO parameters? (y/n)[n]:
>  Will you set power management parameters? (y/n) [n]:
>  Will you set tone blackout configuration parameter? (y/n) [n]:
>  Will you set mode-specific parameters? (y/n) [n]:
  Add profile 10 successfully
```

2. Configure the ADSL2+ channel profile.

   The configuration data in the ADSL2+ channel profile is set according to the actual channel conditions.

```
huawei(config)#adsl channel-profile add 10
  Start adding profile
  Press 'Q' to quit the current configuration and new configuration will be
neglected
>  Do you want to name the profile (y/n) [n]:
>  Will you set the minimum impulse noise protection? (y/n) [n]:y
>    Minimum impulse noise protection downstream:
>    1-noProtection    2-halfSymbol      3-singleSymbol     4-twoSymbols
>    5-threeSymbols    6-fourSymbols     7-fiveSymbols      8-sixSymbols
>    9-sevenSymbols    10-eightSymbols   11-nineSymbols     12-tenSymbols
>    13-elevenSymbols  14-twelveSymbols  15-thirteenSymbols 16-fourteenSymbols
>    17-fifteenSymbols 18-sixteenSymbols
>    Please select (1~18) [2]:4
>    Minimum impulse noise protection upstream:
>    1-noProtection    2-halfSymbol      3-singleSymbol     4-twoSymbols
>    5-threeSymbols    6-fourSymbols     7-fiveSymbols      8-sixSymbols
>    9-sevenSymbols    10-eightSymbols   11-nineSymbols     12-tenSymbols
>    13-elevenSymbols  14-twelveSymbols  15-thirteenSymbols 16-fourteenSymbols
>    17-fifteenSymbols 18-sixteenSymbols
>    Please select (1~18) [2]:4
>  Will you set interleaving delay parameters? (y/n) [n]:y
>    Maximum interleaving delay downstream (0~63 ms) [16]:24
>    Maximum interleaving delay upstream (0~63 ms) [6]:12
>  Will you set parameters for rate? (y/n) [n]:y
>    Minimum transmit rate downstream (32~32000 Kbps) [32]:
>    Minimum reserved transmit rate downstream (32~32000 Kbps) [32]:
>    Maximum transmit rate downstream (32~32000 Kbps) [24544]:8000
>    Minimum transmit rate upstream (32~6000 Kbps) [32]:
>    Minimum reserved transmit rate upstream (32~6000 Kbps) [32]:
>    Maximum transmit rate upstream (32~6000 Kbps) [1024]:
>  Will you set rate thresholds? (y/n) [n]:
  Add profile 10 successfully
```


Copyright © Huawei Technologies Co., Ltd.

3. Configure the ADSL2+ line template.

   Bind the configured line profile and channel profile together to form line template 10.

```
huawei(config)#adsl line-template add 10
  Start adding template
  Press 'Q' to quit the current configuration and new configuration will be
neglected
>  Do you want to name the template (y/n) [n]:
>  Please set the line-profile index (1~128) [1]:10
>  Will you set channel configuration parameters? (y/n) [n]:y
>    Please set the channel number (1~2) [1]:1
>    Channel1 configuration parameters:
>    Please set the channel-profile index (1~128) [1]:10
Add template 10 successfully
```

4. Configure the ADSL2+ alarm profile.

   You can configure the ADSL2+ alarm profile based on your own needs. For details, see "Configuring an ADSL2+ Alarm Template." In this example, the default alarm profile (template 1) is used.

5. Configure the ADSL2+ traffic profile.

   To configure the ADSL2+ traffic profile, run the **traffic table ip** command.

   In this example, the default profile (profile 6) is used.

6. Activate the ADSL2+ port.

```
huawei(config)#interface adsl 0/2
huawei(config-if-adsl-0/2)#deactivate all
huawei(config-if-adsl-0/2)#alarm-config all 1
huawei(config-if-adsl-0/2)#activate all 1
huawei(config-if-adsl-0/2)#quit
```

7. Configure the upstream port.

   - Configure the GIU board.

     By default, the GE optical port of the GIU board works in the full duplex mode with the rate of 1000 Mbit/s.

     To change the port working mode and the port rate, run the **speed** and **duplex** commands in GIU mode.

     The settings must be the same as the settings of the peer device.

   - Configure the VLAN.

     The ADSL2+ users of MA5600T-1 use the VLAN authentication. In this case, the MUX VLAN is used to identify the users.

```
huawei(config)#vlan 3030 smart
huawei(config)#port vlan 3030 0/19 0
```

8. Add the service port.

   All ports of in slot 0/2 provide the ADSL2+ service. To add service ports in batches, run the **multi-service-port** command.

```
huawei(config)#multi-service-port vlan 3030 port 0/3 0-31 vpi 0 vci 35 user-
encap
 pppoe rx-cttr 6 tx-cttr 6
```

Step 7 Configure the SHDSL service.

The MA5600T supports the SHDSL service of multiple encapsulation modes, such as IPoA, PPPoA, IPoE, and PPPoE. This topic uses the PPPoE mode as an example to describe how to configure the SHDSL service. For other encapsulation modes, see "**3.1 Example: Configuring the xDSL Internet Access Service**."

Copyright © Huawei Technologies Co., Ltd.

1. Configure the SHDSL line profile.

   To configure the SHDSL line profile, run the **shdsl line-profile add** or **shdsl line-profile quickadd** command.

```
huawei(config)#shdsl line-profile quickadd 10 line two-wire rate 2048 2048 psd
 symmetric transmission Annex-A remote disable probe disable snr-margin ds-
curr 10 ds-worst
 10 us-curr 10 us-worst 10 bitmap 0x03
```

2. Configure the SHDSL alarm profile.

   To configure the SHDSL alarm profile, run the **shdsl alarm-profile add** command.

   In this example, the default profile (profile 1) is used.

3. Configure the SHDSL traffic profile.

   To configure the SHDSL traffic profile, run the **traffic table ip** command.

   In this example, the default profile (profile 6) is used.

4. Activate the SHDSL port.

```
huawei(config)#interface shl 0/5
huawei(config-if-shdsl-0/5)#deactivate all
huawei(config-if-shdsl-0/5)#alarm-config all 1
huawei(config-if-shdsl-0/5)#activate all 10
huawei(config-if-shdsl-0/5)#quit
```

5. Configure the upstream port.

   The SHDSL users of MA5600T-3 use the PPPoE authentication. In this case, the smart VLAN is used to identify the users.

```
huawei(config)#vlan 3030 smart
huawei(config)#port vlan 3030 0/19 0-1
  It will take several minutes, and console may be timeout, please use
command
idle-timeout to set time
limit
  Are you sure to add standard port(s)? (y/n)[n]:y
```

6. Add the service port.

   - Ports 0-15 of SHDSL board 0/5 provide the SHDSL service.
   - To add service ports in batches, run the **multi-service-port** command.

```
huawei(config)#multi-service-port vlan 3030 port 0/5 0-15 vpi 0 vci 35 user-
encap
 pppoe rx-cttr 6 tx-cttr 6
```

Step 8 Configure the GPON service.

1. Configure the service VLAN and the upstream port.

```
huawei(config)#vlan 1530 smart
huawei(config)#port vlan 1530 0/19 0
```

2. Configure the DBA profile.

```
huawei(config)#tcont-profile add profile-id 10 type1 fix 102400
```

3. Configure the alarm threshold profile.

   - When you need to configure the alarm threshold value to monitor the performance statistics of the activated ONT line, run the **gpon alarm-profile add** command to configure the GPON alarm threshold profile.
   - In the default GPON alarm threshold profile 1, all alarm thresholds are set to 0, which indicates that no alarm is reported.

Copyright © Huawei Technologies Co., Ltd.

- In this example, the default alarm threshold profile is used. You do not need to configure it.

4. Configure the GPON traffic profile.

```
huawei(config)#traffic table ip index 8 cir 10240 priority 0 priority-policy
tag-In-Package
```

5. Add an ONT.

NOTE

- You can add an ONT in two ways: run the **ont add** command to add an ONT offline or run the **ont confirm** command to confirm an ONT that is in the auto-find state.
- You need to run the **port ont-auto-find** command in the GPON mode to enable the auto-find function of the ONT.

```
huawei(config)#interface gpon 0/18
huawei(config-if-gpon-0/18)#ont add 1 0 hwhw-10101010 password-auth huawei
profile-id 2
```

6. Bind the alarm threshold profile.

```
huawei(config-if-gpon-0/18)#ont alarm-profile 1 0 profile-id 1
```

7. Bind the DBA profile.

```
huawei(config-if-gpon-0/18)#tcont bind-profile 1 0 1 profile-id 10
```

8. Divide the ONT port VLAN.

```
huawei(config-if-gpon-0/18)#ont port vlan 1 0 eth 10 0
huawei(config-if-gpon-0/18)#ont port native-vlan 1 0 eth 0 vlan 1530
```

9. Configure the GEM port.

```
huawei(config-if-gpon-0/18)#gemport add 1 gemportid 150 eth
```

10. Bind the GEM port to an ONT T-CONT.

NOTE

In the actual application, if the ONT terminal does not support the priority queue scheduling, you can use the CAR to limit the rate when binding the GEM port to the ONT T-CONT.

```
huawei(config-if-gpon-0/18)#ont gemport bind 1 0 150 1 priority-queue 3
```

11. Create the mapping between the GEM port and the service stream.

```
huawei(config-if-gpon-0/18)#ont gemport mapping 1 0 150 vlan 1530
huawei(config-if-gpon-0/18)#quit
```

12. Add the service port.

```
huawei(config)#service-port vlan 1530 gpon 0/18/0 gemport 150 multi-service
user-vlan 10 rx-cttr 5 tx-cttr 8
```

Step 9 Configure the POTS service.

1. Configure the upstream ports of the media stream and the signaling flow.

```
huawei(config)#vlan 1600 smart
huawei(config)#interface vlanif 1600
huawei(config)#port vlan 1600 0/19 0
huawei(config-if-vlanif1600)#ip address 10.176.6.33 24
```

2. Configure the static route destined to the MGC.

NOTE

When the MGC and the MG are in the same network segment, you do not need to configure the static route.

```
huawei(config)#ip route-static 10.30.80.0 255.255.255.0 10.176.6.62
```

3. Configure the media IP address pool and the signaling IP address pool.

Copyright © Huawei Technologies Co., Ltd.

```
huawei(config)#voip
huawei(config-voip)#ip address media 10.176.6.33 10.176.6.62
huawei(config-voip)#ip address signaling 10.176.6.33
```

4. Configure the MG interface.

   Add an MG interface.

   ```
   huawei(config)#interface h248 0
     Are you sure to add MG interface? (y/n)[n]:y
   ```

   Configure the MG interface attributes.

   ```
   huawei(config-if-h248-0)#if-h248 attribute mgip 10.176.6.33 mgport 2944 code
   text
    transfer udp mgcip_1 10.30.80.65 mgcport_1 2944 mg-media-ip 10.176.6.33
   ```

   Configure the software parameters of the MG interface (in this example, only parameter 20 is configured, and other parameters use the default values).

   ```
   huawei(config-if-h248-0)#mg-software parameter 20 2
   ```

5. Reset the MG interface.

   NOTE

   After configuring the MG interface, you need to reset the interface to validate the configuration.

   ```
   huawei(config-if-h248-0)#reset coldstart
     Are you sure to reset MG interface?(y/n)[n]:y
   ```

6. Add PSTN users in batches.

   ```
   huawei(config)#esl user
   huawei(config-esl-user)#mgpstnuser batadd 0/3/0 0/3/31 0 terminalid 0 telno
   88660000
   ```

Step 10 Configure the multicast service.

After the configuration, the following results should be achieved:

- Users of port 0/2/2 need to be authenticated, and have rights to watch two programs and to preview one program.
- Users of port 0/2 do not need to be authenticated.

1. Configure the xDSL.

   In this example, it is unnecessary to configure the xDSL. The default line profile (profile 1002) is used.

2. Configure the VLAN.

   - Create a smart VLAN.
     ```
     huawei(config)#vlan 100 smart
     ```
   - Set the VLAN upstream port.
     ```
     huawei(config)#port vlan 100 0/19 0
     ```
   - Configure the native VLAN.
     ```
     huawei(config)#interface giu 0/19
     huawei(config-if-giu-0/19)#native-vlan 0 vlan 100
     ```
   - Create the traffic profile.
     ```
     huawei(config)#traffic table ip index 8 cir off priority 5 priority-policy
     tag-I
     n-Packag
     ```
   - Add ADSL2+ port 2 and 3 to VLAN 100.
     ```
     huawei(config)#service-port vlan 100 adsl 0/2/2 vpi 0 vci 35 rx-cttr 8 tx-
     cttr 8
     huawei(config)#service-port vlan 100 adsl 0/2/3 vpi 0 vci 35 rx-cttr 8 tx-
     cttr 8
     ```


Copyright © Huawei Technologies Co., Ltd.

3. Configure the multicast service

- Enable the multicast proxy function.

```
huawei(config)#multicast-vlan 100
huawei(config-mvlan100)#igmp mode proxy
  Are you sure to change IGMP mode?(y/n)[n]:y
```

- Configure the upstream port.

```
huawei(config-mvlan100)#igmp uplink-port 0/19/0 100
huawei(config-mvlan100)#quit
huawei(config)#btv
huawei(config-btv)#igmp uplink-port-mode default
Are you sure to change the uplink port mode?(y/n)[n]:y
```

- Configure the preview parameters.

  In this example, set the preview duration for program 1 to 150s, the number of preview attempts to 6 each day, and the preview interval to 60s.

```
huawei(config-btv)#igmp preview-profile add index 1 duration 150 times 6
interval 60
huawei(config-btv)#igmp preview auto-reset-time 00:00:00
huawei(config-btv)#quit
```

- Configure the program library.

```
huawei(config)#multicast-vlan 100
huawei(config-mvlan100)#igmp program add name program1 ip 224.1.1.1
sourceip 10.10.10.10
huawei(config-mvlan100)#igmp program add name program2 ip 224.1.1.2
sourceip 10.10.10.10
huawei(config-mvlan100)#igmp program add name program3 ip 224.1.1.3
sourceip 10.10.10.10 preview-profile 1
huawei(config-mvlan100)#quit
```

- Configure the authority profile.

```
huawei(config)#btv
huawei(config-btv)#igmp profile add profile-name profile0
huawei(config-btv)#igmp profile profile-name profile0 program-name program1
watch
huawei(config-btv)#igmp profile profile-name profile0 program-name program2
watch
huawei(config-btv)#igmp profile profile-name profile0 program-name program3
preview
```

- Configure the multicast user.

```
huawei(config-btv)#igmp user add port 0/2/3 no-auth
huawei(config-btv)#igmp user add port 0/2/2 auth
huawei(config-btv)#igmp user bind-profile port 0/2/16 profile-name profile0
huawei(config-btv)#quit
huawei(config)#multicast-vlan 100
huawei(config-mvlan100)#igmp multicast-vlan member port 0/2/2
huawei(config-mvlan100)#igmp multicast-vlan member port 0/2/3
huawei(config-btv)#quit
```

Step 11 Save the data.

```
huawei(config)#save
```

----End

7.6 Configuring MA5600T-4

This topic describes how to configure MA5600T-4.

Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Confirm the board.

```
huawei>enable
huawei#config
huawei(config)#board confirm 0
```

Step 2 Configure the NMS.

1. Configure the IP address of the inband NMS interface.
   - Create the NMS VLAN.
     ```
     huawei(config)#vlan 10 standard
     ```
   - Add the upstream port.
     ```
     huawei(config)#port vlan 10 0/19 0
     ```
   - Enter the NMS VLAN interface mode.
     ```
     huawei(config)#interface vlanif 10
     ```
   - Configure the IP address of the NMS interface.
     ```
     huawei(config-if-vlanif10)#ip address 10.10.1.5 255.255.255.0
     ```
2. Add the route.
   - Configure the route destined to the NMS (Trap destination address).
     ```
     huawei(config)#ip route-static 2.2.2.2 255.255.255.255 10.10.1.1
     preference 1
     huawei(config)#ip route-static 2.2.2.3 255.255.255.255 10.10.1.1
     preference 1
     ```
   - Configure the route destined to the time server.
     ```
     huawei(config)#ip route-static 4.4.4.4 255.255.255.255 10.10.1.1
     preference 1
     huawei(config)#ip route-static 4.4.4.5 255.255.255.255 10.10.1.1
     preference 1
     ```
   - Configure the route destined to the log host.
     ```
     huawei(config)#ip route-static 3.3.3.3 255.255.255.255 10.10.1.1
     preference 1
     huawei(config)#ip route-static 3.3.4.3 255.255.255.255 10.10.1.1
     preference 1
     ```
3. Add the ACL rule.
   ```
   huawei(config)#acl 3050
   huawei(config-acl-adv-3050)#rule permit ip source any destination any
   huawei(config-acl-adv-3050)#rule deny ip source any destination 10.10.1.2
   0.0.0.0
   huawei(config-acl-adv-3050)#rule permit ip source 2.2.2.2 0.0.0.0
   destination 10.10.1.2 0.0.0.0
   huawei(config-acl-adv-3050)#rule permit ip source 2.2.2.3 0.0.0.0
   destination 10.10.1.2 0.0.0.0
   huawei(config-acl-adv-3050)#rule permit ip source 4.4.4.4 0.0.0.0
   destination 10.10.1.2 0.0.0.0
   huawei(config-acl-adv-3050)#rule permit ip source 4.4.4.5 0.0.0.0
   destination 10.10.1.2 0.0.0.0
   huawei(config-acl-adv-3050)#rule permit ip source 3.3.3.3 0.0.0.0
   destination 10.10.1.2 0.0.0.0
   huawei(config-acl-adv-3050)#rule permit ip source 3.3.4.3 0.0.0.0
   destination 10.10.1.2 0.0.0.0
   huawei(config-acl-adv-3050)#quit
   huawei(config)#packet-filter inbound ip-group 3050 port 0/19/0
   huawei(config)#packet-filter inbound ip-group 3050 port 0/19/1
   ```
4. Configure SNMP.
   - Set the community name and access authority.
     ```
     huawei(config)#snmp-agent community read public
     huawei(config)#snmp-agent community write private
     ```


Copyright © Huawei Technologies Co., Ltd.

- Set the SysContact.
  ```
  huawei(config)#snmp-agent sys-info contact HW-075512345678
  ```
- Set the SysLocation.
  ```
  huawei(config)#snmp-agent sys-info location Shenzhen China
  ```
- Set the SNMP version.

  The SNMP version must be the same as the SNMP version of the NMS. In this example, the SNMP version is set as SNMP V2C.

  ```
  huawei(config)#snmp-agent sys-info version v2c
  ```

5. Enable the trap sending.
   ```
   huawei(config)#snmp-agent trap enable standard
   ```
6. Set trap destination address.
   ```
   huawei(config)#snmp-agent target-host trap-hostname huawei address 2.2.2.2
   trap-paramsname abc
   huawei(config)#snmp-agent target-host trap-hostname huawei123 address 2.2.2.3
   trap-paramsname 123
   ```
7. Set the trap source address.
   ```
   huawei(config)#snmp-agent trap source vlanif 10
   ```

Step 3 Configure the time server.

```
huawei(config)#ntp-service unicast-server 4.4.4.4 source-interface vlanif 10
huawei(config)#ntp-service unicast-server 4.4.4.5 source-interface vlanif 10
```

Step 4 Configure the log host.

```
huawei(config)#loghost add 3.3.3.3 syslog-1
huawei(config)#loghost activate ip 3.3.3.3
huawei(config)#loghost add 3.3.4.3 syslog-2
huawei(config)#loghost activate ip 3.3.4.3
```

Step 5 Configure the EMU.

This topic uses the fan monitoring as an example to show how to configure the EMU.

By default, the default slave node number of the fan EMU is 0. In this example, assume that the slave node number is 1. In this case, you need to set the DIP switch of the node address on the fan monitoring unit as 1.

```
huawei(config)#emu add 0 h801ESC 0 0
huawei(config)#emu add 1 fan 0 1
```

Step 6 Configure the VDSL2 service.

The MA5600T supports the VDSL2 Internet service of multiple encapsulation modes, such as IPoA, PPPoA, IPoE, and PPPoE. This topic uses the PPPoE mode as an example to describe how to configure the VDSL2 service. For other encapsulation modes, see "**3.1 Example: Configuring the xDSL Internet Access Service**."

1. Configure the VDSL2 line profile.

   You can configure the VDSL2 line profile based on your requirements.

   ```
   huawei(config)#vdsl line-profile add 10
     Start adding profile
     Press 'Q' to quit the current configuration and new configuration will
   be
   neglected
   >  Do you want to name the profile (y/n) [n]:
   >    Transmission mode:
   >      0: Custom
   >      1: All (G992.1~5,T1.413,G993.2)
   >      2: Full rate(G992.1/3/5,T1.413,G993.2)
   ```


Copyright © Huawei Technologies Co., Ltd.

```
>      3: G.DMT (G992.1/3/5,G993.2)
>      4: G.HS (G992.1~5,G993.2)
>      5: ADSL (G.992.1~5,T1.413)
>      6: VDSL (G993.2)
>    Please select (0~6) [1]:
>  Please select the form of transmit rate adaptation downstream:
>  1-fixed 2-adaptAtStartup (1~2) [2]:
>  Please select the form of transmit rate adaptation upstream:
>  1-fixed 2-adaptAtStartup (1~2) [2]:
>  Will you set SNR margin parameters? (y/n) [n]:
>  Will you set DPBO parameters? (y/n)[n]:
>  Will you set UPBO parameters? (y/n)[n]:
>  Will you set RFI notch configuration parameter? (y/n) [n]:
>  Will you set ADSL tone blackout configuration parameter? (y/n) [n]:
>  Will you set VDSL tone blackout configuration parameter? (y/n) [n]:
>  Will you set mode-specific parameters? (y/n) [n]:
  Add profile 10 successfully
```

2. Configure the VDSL2 channel profile.

   You can configure the VDSL2 channel profile based on your requirements.

```
huawei(config)#vdsl channel-profile add 10
  Start adding profile
  Press 'Q' to quit the current configuration and new configuration will be
neglected
>  Do you want to name the profile (y/n) [n]:
>  Data path mode 1-ATM, 2-PTM, 3-Both (1~3) [3]:1
>  Will you set the minimum impulse noise protection? (y/n) [n]:y
>    Minimum impulse noise protection downstream:
>    1-noProtection    2-halfSymbol      3-singleSymbol     4-twoSymbols
>    5-threeSymbols    6-fourSymbols     7-fiveSymbols      8-sixSymbols
>    9-sevenSymbols    10-eightSymbols   11-nineSymbols     12-tenSymbols
>    13-elevenSymbols  14-twelveSymbols  15-thirteenSymbols 16-
fourteenSymbols
>    17-fifteenSymbols 18-sixteenSymbols
>    Please select (1~18) [1]:3
>    Minimum impulse noise protection upstream:
>    1-noProtection    2-halfSymbol      3-singleSymbol     4-twoSymbols
>    5-threeSymbols    6-fourSymbols     7-fiveSymbols      8-sixSymbols
>    9-sevenSymbols    10-eightSymbols   11-nineSymbols     12-tenSymbols
>    13-elevenSymbols  14-twelveSymbols  15-thirteenSymbols 16-
fourteenSymbols
>    17-fifteenSymbols 18-sixteenSymbols
>    Please select (1~18) [1]:3
>  Will you set interleaving delay parameters? (y/n) [n]:y
>    Maximum interleaving delay downstream (0~200 ms) [20]:
>    Maximum interleaving delay upstream (0~200 ms) [20]:
>  Will you set parameters for rate? (y/n) [n]:y
>    Minimum transmit rate downstream (128~100000 Kbps) [128]:512
>    Maximum transmit rate downstream (512~100000 Kbps) [100000]:
>    Minimum transmit rate upstream (128~100000 Kbps) [128]:
>    Maximum transmit rate upstream (128~100000 Kbps) [100000]:
  Add profile 10 successfully
```

3. Configure the VDSL2 line template.

   Bind the preceding configured line profile and the channel profile together in the line template with the index of 10.

```
huawei(config)#vdsl line-template add 10
  Start adding template
  Press 'Q' to quit the current configuration and new configuration will be
neglected
>  Do you want to name the template (y/n) [n]:
>  Please set the line-profile index (1~128) [1]:10
>  Will you set channel configuration parameters? (y/n) [n]:y
>    Please set the channel number (1~2) [1]:
>    Channel1 configuration parameters:
```


Copyright © Huawei Technologies Co., Ltd.

```
>    Please set the channel-profile index (1~128) [1]:10
  Add template 10 successfully
```

4. Configure the VDSL2 alarm profile.

   You can configure the VDSL2 alarm profile based on your requirements. For the configuration, see "Configuring a VDSL2 Alarm Template". In this example, the default alarm profile 1 is used.

5. Configure the VDSL2 traffic profile.

   You can configure the VDSL2 traffic profile by running the **traffic table ip** command based on your requirements.

   In this example, the default profile (profile 6) is used.

6. Activate the VDSL2 port.

```
huawei(config)#interface vdsl 0/2
huawei(config-if-vdsl-0/2)#alarm-config all
huawei(config-if-vdsl-0/2)#activate all template-index 10
huawei(config-if-vdsl-0/2)#quit
```

7. Configure the upstream port.

   - Configure the GIU board.

     In general, the GE optical port uses the default gigabit full-duplex mode.
     To change the mode, switch to the GIU config mode. Then run the **speed** command to change the port rate, and run the **duplex** command to change the port duplex mode.
     The settings of the upstream port must be the same as the settings on the peer device.

   - Configure the VLAN.

     The VDSL2 users of MA5600T-1 use the PPPoE authentication. In this case, the smart VLAN is used to identify the users.

```
huawei(config)#vlan 1800 smart
huawei(config)#port vlan 1800 0/19 0
```

8. Add the service port.

   All ports in slot 0/2 provide the VDSL2 Internet access service. To add service ports in batches, run the **multi-service-port** command.

```
huawei(config)#multi-service-port vlan 1800 port 0/2 0-23 vpi 0 vci 35 user-encap
 pppoe rx-cttr 6 tx-cttr 6
```

Step 7 Configure the QinQ private line service.

MA5600T-4 and MA5600T-1 serve two branches of a company to provide the QinQ private line service.

1. Create VLAN 50.

```
huawei(config)#vlan 50 mux
```

2. Set VLAN 50 as QinQ VLAN.

```
huawei(config)#vlan attrib 50 q-in-q
```

3. Add the upstream port.

```
huawei(config)#port vlan 50 0/19 0
```

4. Add the service port.

   To add the service port, run the **service-port** command. Note that the VPI and VCI values of the service port must be the same as those on the modem.

Copyright © Huawei Technologies Co., Ltd.

The QinQ VLAN supports the PVC-priority scheduling policy only. In this case, select the profile that supports PVC-priority policy.

```
huawei(config)#service-port vlan 50 shdsl 0/5/15 vpi 0 vci 35
 rx-cttr 7 tx-cttr 7
```

Step 8 Save the data.

```
huawei(config)#save
```

----End

7.7 Verification

All services configured on all DSLAMs run in the normal state.

Copyright © Huawei Technologies Co., Ltd.

8 FTTx Configuration Summary

The Configuration Guide of the FTTx Solution is a set of configurations of FTTx networks, including fiber to the home (FTTH), fiber to the building (FTTB), fiber to the curb (FTTC), fiber to the office (FTTO), fiber to the mobile base station (FTTM), and multiservice operator (MSO). This manual is described according to the following:

Structure of Overview, Data Plan, and Configuration

The description structure of each sub-solution is overview, data plan, and configuration. In this case, you can know about the overview first and then the details, and configure services in actual scenarios.

1. Overview: Describes the basic concepts, scenarios, typical network topologies, and ONU capability set of solutions, providing necessary contexts for users.
2. Data plan: Describes the principle of data plan, providing reference to data configuration.
3. Configuration: Describes the procedure of configuring a service in a network topology and provides the method of verifying the service.

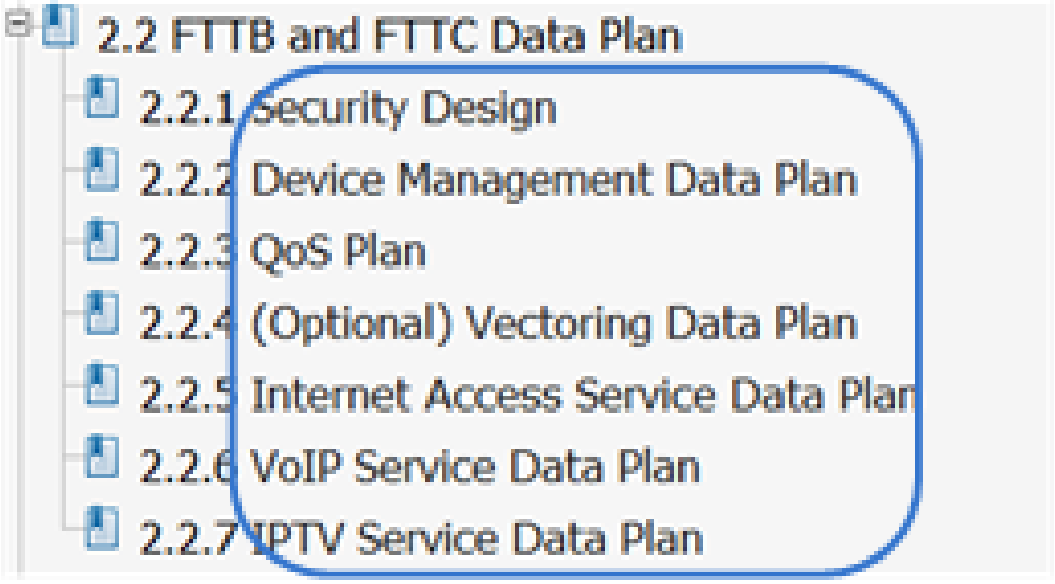
Recommended Principle of Data Plan

Data plan is the key factor and difficulty for network planning engineers and commissioning engineers. This manual provides the recommended principle of data plan for security, device management, QoS, and specific service in various sub-solutions. In this case, you can plan and deploy services efficiently.

Takes the FTTB/C sub-solution as an example, the principle of data plan is shown in **Figure 8-1**.

Copyright © Huawei Technologies Co., Ltd.

Figure 8-1 Recommended Principle of Data Plan

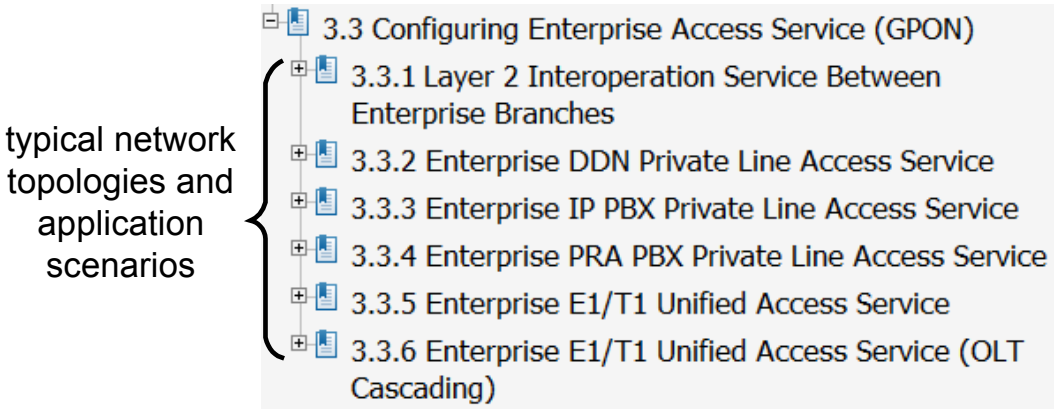


Typical Network Topology and Application Scenario

Various sub-solutions have different features. This manual is described based on the typical network topologies and application scenarios. In this case, you can find out the required contents according to the actual network topology and application scenario.

Takes the Private Line Service Configuration (Enterprise Access) sub-solution as an example, the application scenarios are shown in **Figure 8-2**.

Figure 8-2 Typical Application Scenario



One-button Script Tool

Through a simple-to-use interface, you can instantly transform any configuration page into command scripts, which greatly reduces the probability of errors compared to manually.

Copyright © Huawei Technologies Co., Ltd.

Click to experience: Script Conversion Tool.

Copyright © Huawei Technologies Co., Ltd.

9 FTTH Configuration

About This Chapter

This section describes the configurations of Internet access, voice, broadband TV (BTV), and VoD services in fiber to the home (FTTH) networking scenarios.

9.1 FTTH Service Overview
This topic describes FTTH service from basic concepts, network scenarios, typical configurations, and ONT capability sets to provide necessary background information for FTTH service configuration in different scenarios.

9.2 Basic Concepts
This section describes basic concepts related to the fiber to the home (FTTH) solution from the user side to the network side on FTTH networking using PON and P2P upstream transmission, respectively.

9.3 Networking Scenarios and Hardware Configurations (GPON)
This section describes fiber to the home (FTTH) networking scenarios and hardware configurations of an optical line terminal (OLT) and optical network terminals (ONTs).

9.4 Networking Scenarios and Hardware Configurations (P2P)
This section describes fiber to the home (FTTH) networking scenarios and hardware configurations of an optical line terminal (OLT) and optical network terminals (ONTs).

9.5 Reference of GPON ONT Capability Sets
This topic provides common GPON ONT capability sets of Huawei, serving as a reference for parameter configuration when an ONT is added offline.

9.6 Principle of FTTH Data Plan

9.7 GPON Access: Configuring FTTH Service
This topic describes how to configure the Internet access service, voice service and BTV service and VoD service in GPON access mode in FTTH network scenario.

9.8 P2P Access: Configuring FTTH Service
Users connected to the OLT through an ONT, and are therefore provided with the Internet, VoIP, and IPTV service through a same port.

Copyright © Huawei Technologies Co., Ltd.

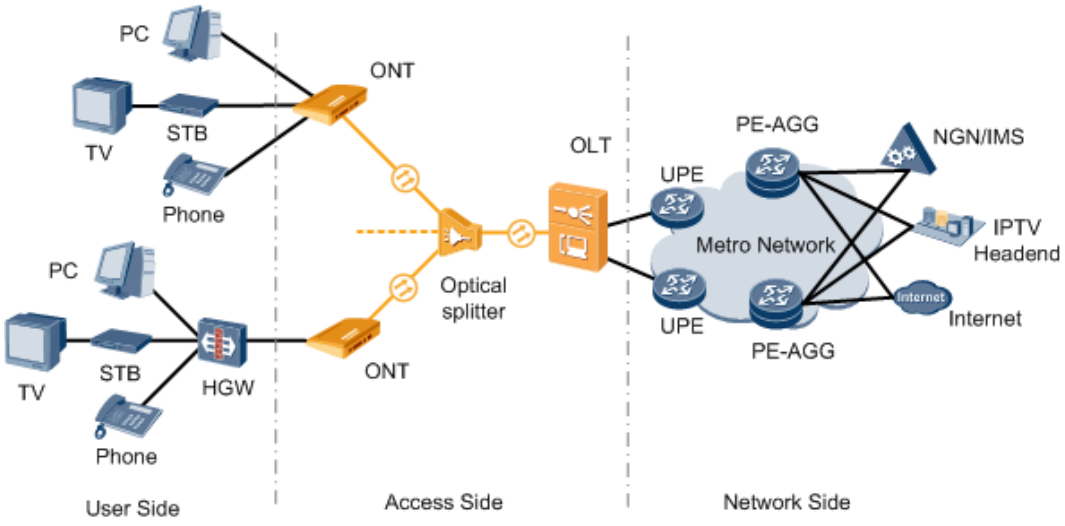
9.1 FTTH Service Overview

This topic describes FTTH service from basic concepts, network scenarios, typical configurations, and ONT capability sets to provide necessary background information for FTTH service configuration in different scenarios.

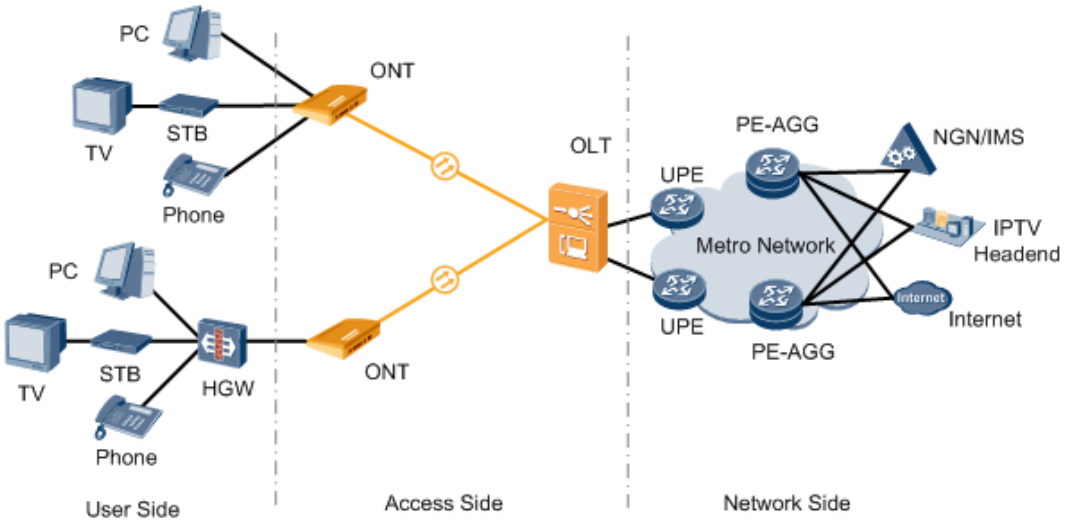
9.2 Basic Concepts

This section describes basic concepts related to the fiber to the home (FTTH) solution from the user side to the network side on FTTH networking using PON and P2P upstream transmission, respectively.

FTTH Networking Using PON Upstream Transmission



FTTH Networking Using P2P Upstream Transmission



Copyright © Huawei Technologies Co., Ltd.

User Side

Concept	Description
Home gateway (HGW or HG)	A gateway device positioned for small office and home office (SOHO) users. It provides multiple service ports, such as POTS and LAN, wireless local area network (WLAN), or xDSL ports. The HGW supports routing and remote management and diagnosis.
VoD	A technology that enables users to order any program in a VoD program library. During program playing, users can perform operations, such as pause, fast forward, fast rewind, and program locating.
Multicast	Is also called broadband TV (BTV), which is similar to traditional cable TV (CATV) or satellite TV. The user experience in watching a multicast program is the same as that in watching a traditional TV program. Unlike the traditional TV, the IPTV system encodes audio signals and sends them to user terminals through an IP network.

Access Side

Concept	Description
PON	A network that uses the point-to-multipoint (P2MP) network architecture. A PON network consists of an optical line terminal (OLT), an optical distribution network (ODN), and optical network units (ONUs). It uses optical fibers to transmit data, supports more users with less optical fibers, and provides high access rates.
ODN	A network that consists of optical fibers and passive optical components, such as one or more optical dividers. The ODN network provides highly reliable optical paths to connect ONUs to an OLT.
OLT	An aggregation device located at a central office (CO), which terminates PON protocols. In this document. OLTs are MA5600T/MA5603T/ MA5608Ts.
Optical network terminal (ONT)	A user terminal that provides various ports for users. In PON networking, the PON board of an OLT communicates with an ONT through the intermediate ODN network. In point-to-point (P2P) networking, an OLT communicates with an ONT through a P2P Ethernet optical access board.
Split ratio	A ratio used for dividing a downstream optical signal into sub-signals in the PON system. A greater split ratio will result in a high optical power for signal transmission over the same physical distance.
Fiber to the home (FTTH)	A type of network that provides high bandwidths for home users. In PON networking, an OLT connects to ONTs through an ODN network and the ONTs connect to home users. In P2P networking, an OLT connects to ONTs and the ONTs connect to home users. The OLT provides voice, Internet access, and IPTV services for home users.

Copyright © Huawei Technologies Co., Ltd.

Network Side

Concept	Description
User-facing provider edge (U-PE)	A supplier routing device that connects to the router of a customer edge (CE), which is an OLT in this document. The U-PE supports routing and Multiprotocol Label Switching (MPLS) encapsulation. If a U-PE connects to multiple CEs, the U-PE supports basic bridging functions. In this case, the U-PE forwards data frames, which reduces the load of switching provider edges (S-PEs).
Aggregation provider edge (PE-AGG)	An aggregation router, which provides aggregation and route forwarding functions for access devices. Compared with U-PEs, PE-AGGs provides fewer ports and higher performance and switching rates.
NGN or IP multimedia subsystem (IMS)	A type of network that centers around softswitches and uses an open and standardized architecture. It provides voice, video, and data services. A type of system that uses Session Initiation Protocol (SIP) signaling as its call control signaling. It provides voice, data, and multimedia services. **NOTE** In this document, the NGN or IMS is the softswitch that supports H.248 or SIP.
IPTV head end	A contents preparation platform in the IPTV system. It receives signals, converts media formats, and manages media materials.

9.3 Networking Scenarios and Hardware Configurations (GPON)

This section describes fiber to the home (FTTH) networking scenarios and hardware configurations of an optical line terminal (OLT) and optical network terminals (ONTs).

Copyright © Huawei Technologies Co., Ltd.

Networking Scenario	Description	OLT Device (Main Control Board +Service Board +Upstream Board)	ONT Device
9.7.1 Bridging +Voice ONT Network Scenario	The ONT integrating an integrated access device (IAD) provides Internet, VoIP, and IPTV services to users. The bridging+voice ONT provides Layer 2 data and voice services. This scenario provides transparent transmission channels and requires simple service configuration, so this scenario applies to Layer 2 networking. ● For data services, a PC directly performs dial-up. Then, the upper-layer broadband remote access server (BRAS) device authenticates and accesses the PC. The PC can also access the Internet using the Dynamic Host Configuration Protocol (DHCP) or static IP address. ● The ONT with a built-in voice module encapsulates voice service packets, and the OLT transmits them to the upstream next generation network (NGN) or IP multimedia subsystem (IMS).	● H801SCUN/ H802SCUN +H805GPBD/ H806GPBH/ H802GPBD +H801GICF/ H801GICG/ H801X2CS ● H801SCUH +HG802GPFD +H801GICD/ H801GICE/ H801X2CS ● H801MCUD +H805GPBD/ H806GPBH/ H802GPBD (no upstream board is configured and H801MCUD is used as the control board for upstream transmission)	For supported ONTs in different scenarios, see **9.5 Reference of GPON ONT Capability Sets**.

Copyright © Huawei Technologies Co., Ltd.

Networking Scenario	Description	OLT Device (Main Control Board +Service Board +Upstream Board)	ONT Device
9.7.2 Bridging ONT + HGW Network Scenario	The HGW integrating an IAD provides Internet, voice over Internet Protocol (VoIP), and Internet Protocol television (IPTV) services to users. Services are implemented on the HGW, and the bridging ONT works with the OLT to provide Layer 2 channels.		
9.7.3 Gateway ONT Network Scenario	The ONT integrating an IAD provides Internet, VoIP, and IPTV services to users. The HGW ONT facilitates interconnection of home devices by providing Layer 3 services, such as Point-to-Point Protocol over Ethernet (PPPoE)/DHCP dial-up, network address translation (NAT), and Internet Group Management Protocol (IGMP) snooping. This scenario provides fine-grained management channels and service control, and applies to Layer 3 networking.		

NOTE

The preceding three networking modes for GPON access services are in non-simplified mode. In simplified mode, the triple play service is used as an example to describe how to configure a GPON access service. For details, see **9.7.4 Configuring Triple Play Service (Simplified Mode)**.

9.4 Networking Scenarios and Hardware Configurations (P2P)

This section describes fiber to the home (FTTH) networking scenarios and hardware configurations of an optical line terminal (OLT) and optical network terminals (ONTs).

Copyright © Huawei Technologies Co., Ltd.

Networking Scenario	Description	OLT Device
9.8 P2P Access: Configuring FTTH Service	The P2P Ethernet optical access board of an OLT connects to ONTs to provide voice, Internet access, and IPTV services for users.	Service board: H801OPFA/ H802OPGD/H802OPGE

9.5 Reference of GPON ONT Capability Sets

This topic provides common GPON ONT capability sets of Huawei, serving as a reference for parameter configuration when an ONT is added offline.

ONT Type	Product Name	User-to-Network Interface (UNI)	Number of GEM Ports	IP Address Configured Capability	Number of T-CONTs	Mapping Mode Between Service Streams and the GEM Port	Flow Control Type	Number of PQs Supported by a T-CONT
Bridging	HG810	1ETH	32	Not supported	8	VLAN/ PRI/ VLAN +PRI	PQ/ Gemport CAR	T-CONT 0:3 T-CONT 1-7:4
	HG810a	1ETH	32	Not supported	8	VLAN/ PRI/ VLAN +PRI	PQ/ Gemport CAR	T-CONT 0:3 T-CONT 1-7:4

Copyright © Huawei Technologies Co., Ltd.

ONT Type	Product Name	User-to-Network Interface (UNI)	Number of GEM Ports	IP Address Configured Capability	Number of T-CONTs	Mapping Mode Between Service Streams and the GEM Port	Flow Control Type	Number of PQs Supported by a T-CONT
	HG8010	1GE	32	Supported	8	VLAN/PRI/VLAN+PRI/IPToS/Port/Port+VLAN/Port+PRI/Port+VLAN+PRI	PQ/Gemport CAR/Flow CAR	4
	HG8010H	1GE	32	Supported	8	VLAN/PRI/VLAN+PRI/IPToS/Port/Port+VLAN/Port+PRI/Port+VLAN+PRI	PQ/Gemport CAR/Flow CAR	8

Copyright © Huawei Technologies Co., Ltd.

ONT Type	Product Name	User-to-Network Interface (UNI)	Number of GEM Ports	IP Address Configured Capability	Number of T-CONTs	Mapping Mode Between Service Streams and the GEM Port	Flow Control Type	Number of PQs Supported by a T-CONT
	HG8012	1GE+1RF	32	Supported	8	VLAN/PRI/VLAN+PRI/IPToS/Port/Port+VLAN/Port+PRI/Port+VLAN+PRI	PQ/Gemport CAR/Flow CAR	8
	HG8040H	4GE	32	Supported	8	VLAN/PRI/VLAN+PRI/IPToS/Port/Port+VLAN/Port+PRI/Port+VLAN+PRI	PQ/Gemport CAR/Flow CAR	8

Copyright © Huawei Technologies Co., Ltd.

ONT Type	Product Name	User-to-Network Interface (UNI)	Number of GEM Ports	IP Address Configured Capability	Number of T-CONTs	Mapping Mode Between Service Streams and the GEM Port	Flow Control Type	Number of PQs Supported by a T-CONT
Bridging +voice	HG8110	1POTS+1GE	32	Supported	8	VLAN/PRI/ VLAN+PRI/ IPToS/ Port/ Port+VLAN/Port+PRI/ Port+VLAN+PRI	PQ/ Gemport CAR/ Flow CAR	4
	HG8110H	1POTS+1GE	32	Supported	8	VLAN/PRI/ VLAN+PRI/ IPToS/ Port/ Port+VLAN/Port+PRI/ Port+VLAN+PRI	PQ/ Gemport CAR/ Flow CAR	8

Copyright © Huawei Technologies Co., Ltd.

ONT Type	Product Name	User-to-Network Interface (UNI)	Number of GEM Ports	IP Address Configured Capability	Number of T-CONTs	Mapping Mode Between Service Streams and the GEM Port	Flow Control Type	Number of PQs Supported by a T-CONT
	HG8240	2POTS+4GE	32	Supported	8	VLAN/PRI/VLAN+PRI/IPToS/Port/Port+VLAN/Port+PRI/Port+VLAN+PRI	PQ/Gemport CAR/Flow CAR	4
	HG8240B	2POTS+4GE	32	Supported	8	VLAN/PRI/VLAN+PRI/IPToS/Port/Port+VLAN/Port+PRI/Port+VLAN+PRI	PQ/Gemport CAR/Flow CAR	4

Copyright © Huawei Technologies Co., Ltd.

ONT Type	Product Name	User-to-Network Interface (UNI)	Number of GEM Ports	IP Address Configured Capability	Number of T-CONTs	Mapping Mode Between Service Streams and the GEM Port	Flow Control Type	Number of PQs Supported by a T-CONT
	HG8240F	2POTS+4FE	32	Supported	8	VLAN/PRI/VLAN+PRI/IPToS/Port/Port+VLAN/Port+PRI/Port+VLAN+PRI	PQ/Gemport CAR/Flow CAR	4
	HG8240H	2POTS+4GE	32	Supported	8	VLAN/PRI/VLAN+PRI/IPToS/Port/Port+VLAN/Port+PRI/Port+VLAN+PRI	PQ/Gemport CAR/Flow CAR	8

Copyright © Huawei Technologies Co., Ltd.

ONT Type	Product Name	User-to-Network Interface (UNI)	Number of GEM Ports	IP Address Configured Capability	Number of T-CONTs	Mapping Mode Between Service Streams and the GEM Port	Flow Control Type	Number of PQs Supported by a T-CONT
	HG8242	2POTS+4GE+1RF	32	Supported	8	VLAN/PRI/VLAN+PRI/IPToS/Port/Port+VLAN/Port+PRI/Port+VLAN+PRI	PQ/Gemport CAR/Flow CAR	4
Gateway	HG8240A	2POTS+4FE	32	Supported	8	VLAN/PRI/VLAN+PRI/IPToS/Port/Port+VLAN/Port+PRI/Port+VLAN+PRI	PQ/Gemport CAR/Flow CAR	4

Copyright © Huawei Technologies Co., Ltd.

ONT Type	Product Name	User-to-Network Interface (UNI)	Number of GEM Ports	IP Address Configured Capability	Number of T-CONTs	Mapping Mode Between Service Streams and the GEM Port	Flow Control Type	Number of PQs Supported by a T-CONT
	HG8240R	2POTS+4FE	32	Supported	8	VLAN/PRI/VLAN+PRI/IPToS/Port/Port+VLAN/Port+PRI/Port+VLAN+PRI	PQ/Gemport CAR/Flow CAR	T-CONT 0: 3 T-CONT 1-7: 4
	HG8245	2POTS+4GE+USB+WiFi	32	Supported	8	VLAN/PRI/VLAN+PRI/IPToS/Port/Port+VLAN/Port+PRI/Port+VLAN+PRI	PQ/Gemport CAR/Flow CAR	T-CONT 0: 3 T-CONT 1-7: 4

Copyright © Huawei Technologies Co., Ltd.

ONT Type	Product Name	User-to-Network Interface (UNI)	Number of GEM Ports	IP Address Configured Capability	Number of T-CONTs	Mapping Mode Between Service Streams and the GEM Port	Flow Control Type	Number of PQs Supported by a T-CONT
	HG8245A	2POTS+4FE+USB+WiFi	32	Supported	8	VLAN/PRI/VLAN+PRI/IPToS/Port/Port+VLAN/Port+PRI/Port+VLAN+PRI	PQ/Gemport CAR/Flow CAR	4
	HG8245H	2POTS+4GE+USB+WiFi	32	Supported	8	VLAN/PRI/VLAN+PRI/IPToS/Port/Port+VLAN/Port+PRI/Port+VLAN+PRI	PQ/Gemport CAR/Flow CAR	8

Copyright © Huawei Technologies Co., Ltd.

ONT Type	Product Name	User-to-Network Interface (UNI)	Number of GEM Ports	IP Address Configured Capability	Number of T-CONTs	Mapping Mode Between Service Streams and the GEM Port	Flow Control Type	Number of PQs Supported by a T-CONT
	HG8245Q	2POTS+4GE+2USB+2.4G&5GWiFi	32	Supported	8	VLAN/PRI/VLAN+PRI/IPToS/Port/Port+VLAN/Port+PRI/Port+VLAN+PRI	PQ/Gemport CAR/Flow CAR	8
	HG8245T	2POTS+4GE+USB+WiFi	32	Supported	8	VLAN/PRI/VLAN+PRI/IPToS/Port/Port+VLAN/Port+PRI/Port+VLAN+PRI	PQ/Gemport CAR/Flow CAR	4

Copyright © Huawei Technologies Co., Ltd.

ONT Type	Product Name	User-to-Network Interface (UNI)	Number of GEM Ports	IP Address Configured Capability	Number of T-CONTs	Mapping Mode Between Service Streams and the GEM Port	Flow Control Type	Number of PQs Supported by a T-CONT
	HG8247	2POTS+4GE+USB+RF+WiFi	32	Supported	8	VLAN/PRI/VLAN+PRI/IPToS/Port/Port+VLAN/Port+PRI/Port+VLAN+PRI	PQ/Gemport CAR/Flow CAR	4
	HG8247T	2POTS+4GE+USB+RF+WiFi	32	Supported	8	VLAN/PRI/VLAN+PRI/IPToS/Port/Port+VLAN/Port+PRI/Port+VLAN+PRI	PQ/Gemport CAR/Flow CAR	4

Copyright © Huawei Technologies Co., Ltd.

ONT Type	Product Name	User-to-Network Interface (UNI)	Number of GEM Ports	IP Address Configured Capability	Number of T-CONTs	Mapping Mode Between Service Streams and the GEM Port	Flow Control Type	Number of PQs Supported by a T-CONT
	HG8447	4POTS+4GE+USB+RF+WiFi	32	Supported	8	VLAN/PRI/VLAN+PRI/IPToS/Port/Port+VLAN/Port+PRI/Port+VLAN+PRI	PQ/Gemport CAR/Flow CAR	4

NOTE

When flow control type GEM port CAR is used, upstream QoS does not take effect for both the HG810 and HG810a and therefore packets are not scheduled by priority. As a result, when network congestion occurs, packets with various priorities are not processed by priority but are dropped randomly on the HG810 or HG810a.

9.6 Principle of FTTH Data Plan

9.6.1 Data Plan Principles for IP Addresses

This section describes how to obtain an IP address in various scenarios.

Data Plan Principles for IP Addresses

Terminal Type	Service	Recommended Solution
Bridging+Voice ONT	Internet access	A PC obtains an IP address through PPPoE dialup. The ONT transparently transmits the packets.

Copyright © Huawei Technologies Co., Ltd.

Terminal Type	Service	Recommended Solution
	VoIP	The ONT functions as a DHCP client and obtains an IP address from the DHCP server, or the NMS issues a static IP address to the ONT using the configuration file. Voice signaling and media streams at multiple POTS ports share one IP address. Media streams are distinguished by port.
	IPTV	The set top box (STB) obtains an IP address from the DHCP server for ordering programs. The ONT transparently transmits the packets.
Bridging ONT +HGW	Internet access	The HGW functions as a PPPoE client and obtains an IP address through PPPoE dialup. At the same time, the HGW functions as a DHCP server and allocates IP addresses to PCs through the network cable and wireless fidelity (Wi-Fi) access. The ONT transparently transmits the packets.
	VoIP	The HGW functions as a DHCP client and obtains an IP address from the DHCP server, or the application control server (ACS) issues a static IP address to the HGW using TR069. Voice signaling and media streams at multiple POTS ports share one IP address. Media streams are distinguished by port. The ONT transparently transmits the packets.
	IPTV	The HGW is configured with a bridging WAN port. The STB obtains an IP address from the DHCP server. The HGW transparently transmits packets. The ONT also transparently transmits the packets.
Gateway ONT	Internet access	The HGW functions as a PPPoE client and obtains an IP address through PPPoE dialup. The ONT functions as a DHCP server and allocates IP addresses to PCs through the network cable and WiFi access.
	VoIP	The ONT functions as a DHCP client and obtains an IP address from the DHCP server, or the NMS issues a static IP address to the ONT using the configuration file. Voice signaling and media streams at multiple POTS ports share one IP address. Media streams are distinguished by port.
	IPTV	The ONT functions as a DHCP client and obtains an IP address from the DHCP server. At the same time, the ONT functions as a DHCP server and allocates IP addresses to STBs.

9.6.2 Principle of QoS Planning

The QoS planning is an E2E planning, and it can be divided into following policies: traffic classification, marking, and scheduling policy; and traffic monitoring and DBA policy.

Copyright © Huawei Technologies Co., Ltd.

Traffic Classification, Marking, and Scheduling Policy

Service Type	802.1p Priority	Queue Scheduling Method	OLT Queue ID (8 Queues)	ONT Queue.ID	
				When Eight Queues Are Supported	When Four Queues Are Supported
Management service	6	PQ	6	6	3
VoIP service	5	PQ	5	5	2
IPTV service	4	PQ	4	4	2
Internet access service	0	PQ	0	0	0

Note: The service priorities in this table are the recommended values. The service priorities are arranged according to the operators's actual plan.

Traffic Monitoring and DBA Policy

Items	Management service	Internet access service	VoIP service	IPTV service
GEM port	11 [Remark 1]	12	13	14
TCONT	All services share a T-CONT.			
DBA type	Type 3 (DBA profile: assured bandwidth + maximum bandwidth. Users are allowed to preempt the bandwidth on condition that the users' assured bandwidth is guaranteed. However, the total bandwidth cannot exceed the maximum bandwidth.)			
DBA bandwidth planning	Configure the DBA bandwidth according to the user's bandwidth package. The assured bandwidth is the maximum bandwidth required by management packets, VoIP, and IPTV upstream packets. The maximum bandwidth is larger than or equal to the maximum bandwidth that users apply.			
Rate limit on OLT downstream	No rate limit	Configure rate limit by a traffic profile as required. [Remark 2]	No rate limit	No rate limit

Copyright © Huawei Technologies Co., Ltd.

Items	Management service	Internet access service	VoIP service	IPTV service
Rate limit on ONU upstream port	No rate restriction			
Rate limit on ONU downstream port	No rate restriction			

Remark 1: GEM port value depends on the planning of the service provider, but in principle, use different GEM ports for different services.

Remark 2: **Table 9-1** shows the reference service bandwidth of each service for each user.

Table 9-1 Reference service bandwidth of each service for each user

Service Type	Upstream Bandwidth	Downstream Bandwidth	Bandwidth Description
Internet access service	Determined based on the service tariff package.	Determined based on the service tariff package.	Available bandwidth or Internet access service = Committed bandwidth of the service tariff package - VoIP bandwidth - IPTV bandwidth
VoIP service	200 kbit/s	200 kbit/s	The upstream bandwidth and the downstream bandwidth of VoIP service are symmetrical. The actual bandwidth is related to the coding format. This bandwidth is calculated for two POTS ports.
IPTV service (standard definition program)	/	2.5 Mbit/s per channel	IPTV service mainly occupies the downstream bandwidth. The actual bandwidth depends on the coding format, the picture in picture information, 10% bandwidth burst traffic, and the number of programs that can be concurrently watched by one user (in the case of multiple STBs). The upstream bandwidth is mainly used for transmitting IGMP packets, which requires little bandwidth. Therefore, the bandwidth occupied by IGMP packets can be neglected.

Copyright © Huawei Technologies Co., Ltd.

Service Type	Upstream Bandwidth	Downstream Bandwidth	Bandwidth Description
IPTV service (high definition program)	/	9.7 Mbit/s per channel	

Note:

- The rate restriction on the BRAS or SR is recommended. OLTs and ONTs do not restrict the rate for service streams.
- If BRAS does not support rate restriction, OLTs can restrict the rate for service streams through the traffic profile.
- Different service packets on the ONT are distinguished by different VLAN IDs. The service packets are mapped to GEM ports based on VLAN IDs so that different service packets are transmitted to different GEM ports. Each GEM port (each service) corresponds to a T-CONT or all GEM ports share a T-CONT.
- The sum of the assured bandwidth of all ONTs connected to a PON port and the fixed bandwidth of OMCI management channel is less than the GPON upstream bandwidth. Some bandwidth must be reserved for the future service expansion.

9.6.3 Principle of Internet Access Service Data Plan

The Internet access service plan mainly includes the plan of the VLAN and VLAN translation policy in different network scenarios.

VLAN and VLAN Translation policy.

Application Scenario	VLAN Plan	VLAN Translation Policy
Bridging+Voice ONT	Double-tagged VLAN	ONT: ONTs configure the VLAN and add the same C-VLAN tag to packets. All ONTs are in the same C-VLAN. OLT: The OLT performs VLAN translation: C<->S+C'. The C'-VLAN of every ONT differs from each other.

Copyright © Huawei Technologies Co., Ltd.

Application Scenario	VLAN Plan	VLAN Translation Policy
Bridging ONT + HGW	Double-tagged VLAN	ONT: The upstream packets sent from the HGW carry user-VLANs and the ONT transparently transmits them. OLT: The OLT translates the U-VLAN to S-VLAN+C-VLAN.
Gateway ONT	Double-tagged VLAN	ONT: ONTs configure the VLAN and add the same C-VLAN tag to packets. All ONTs are in the same C-VLAN. OLT: The OLT performs VLAN translation: C<->S+C'. The C'-VLAN of every ONT differs from each other.

Note:

- UserVLAN: VLAN carried by upstream packets of user-side devices, U for short.
- C-VLAN: VLAN added based on the ONT/ONU port. For details, see the description of the Double-tagged VLAN S+C.
- Double-tagged VLAN S+C: C indicates the inner VLAN (C-VLAN) and S indicates the outer VLAN (S-VLAN).
- Double-layer VLAN S+C': C' indicates the translated inner VLAN (C'-VLAN) and S indicates the outer VLAN (SVLAN).
- Single-tagged S-VLAN: Single-tagged VLAN marked or translated by the OLT. It is generally used in a single-tagged VLAN translation scenario.
- C<->S+C': Bidirectional VLAN translation: translates the inner C-VLAN and then adds one outer S-VLAN.
- C<->S+C: Bidirectional VLAN translation: maintains the inner C-VLAN and adds one outer S-VLAN.

NOTE

- To ensure traceability of users and finer-grained QoS control and management of users and services, plan per user per service per VLAN (PUPSPV) for the Internet access service. Considering OLT capacity and VLAN scalability, use dual VLANs (S-VLAN+C-VLAN) on the OLT to differentiate users for the Internet access service.
- The outer S-VLAN, which identifies services and physical location, can be allocated based on the OLT, PON board, or PON port. The inner C-VLAN identifies users. User C-VLANs must be unique in one S-VLAN.
- It is recommended that you use stacking VLANs as S-VLANs so that security features, such as PPPoE+/opton82, and anti MAC attacks and anti spoofing spoofing can be easily deployed.
- The 802.1q in 802.1q (QinQ) VLAN is used in the enterprise private line scenario, such as (TLS). The device transparently transmits packets. It is not recommended that you use QinQ VLANs as S-VLANs for the triple play services of residential users.

Copyright © Huawei Technologies Co., Ltd.

9.6.4 Principle of Voice Service Data Plan

The voice service plan mainly includes the plan of the VLAN and VLAN translation policy in different network scenarios, and the plan of voice protocol.

VLAN and VLAN Translation Policy

Application Scenario	VLAN Plan	VLAN Translation Policy
Bridging+voice ONT	Single-tagged VLAN (recommended)	ONT: VLANs are configured for the ONTs on the same network in a unified manner, and the ONTs have the same C-VLAN. The ONT adds a C-VLAN tag to packets. OLT: transparently transmits the VLAN.
	Double-tagged VLAN	ONT: VLANs are configured for the ONTs on the same network in a unified manner, and the ONTs have the same C-VLAN. The ONT adds a C-VLAN tag to packets. OLT: adds an S-VLAN tag to the packets (C-VLAN <-> S-VLAN+C-VLAN).
	Double-tagged VLAN	ONT: VLANs are configured for the ONTs on the same network in a unified manner, and the ONTs have different C-VLANs. The ONT adds a C-VLAN tag to packets. OLT: adds an S-VLAN tag to the packets (C-VLAN <-> S-VLAN+C-VLAN).
Bridging ONT +HGW	Single-tagged VLAN (recommended)	ONT: Packets that are sent upstream by the HGW are tagged with a user VLAN. The ONT transparently transmits the user VLAN. OLT: translates the VLAN tag (user VLAN <-> S-VLAN).
	Single-tagged VLAN	ONT: Packets that are sent upstream by the HGW are tagged with a user VLAN. The ONT translates the user VLAN (user VLAN <-> S-VLAN). All the ONTs connected to the same OLT have the same voice service S-VLAN; ONTs connected to different OLTs may have different voice service S-VLANs. OLT: transparently transmits the VLAN.

Copyright © Huawei Technologies Co., Ltd.

Application Scenario	VLAN Plan	VLAN Translation Policy
	Double-tagged VLAN	ONT: Packets that are sent upstream by the HGW are tagged with a user VLAN. The ONT transparently transmits the user VLAN. OLT: translates the VLAN tag (user VLAN <-> S-VLAN+C-VLAN).
	Double-tagged VLAN	ONT: Packets that are sent upstream by the HGW are tagged with a user VLAN. The ONT translates the user VLAN (user VLAN <-> C-VLAN). The C-VLAN is an inner VLAN tag that differentiates users. OLT: adds an S-VLAN tag to the packets (C-VLAN <-> S-VLAN+C-VLAN).
Gateway ONT	Single-tagged VLAN (recommended)	ONT: VLANs are configured for the ONTs on the same network in a unified manner, and the ONTs have the same C-VLAN. The ONT adds a C-VLAN tag to packets. OLT: translates the VLAN tag (C-VLAN <-> S-VLAN).
	Single-tagged VLAN	ONT: VLANs are configured for the ONTs on the same network in a unified manner, and the ONTs have the same C-VLAN. The ONT adds a C-VLAN tag to packets. OLT: transparently transmits the VLAN.
	Double-tagged VLAN	ONT: VLANs are configured for the ONTs on the same network in a unified manner, and the ONTs have the same C-VLAN. The ONT adds a C-VLAN tag to packets. OLT: translates the VLAN tag (C-VLAN <-> S-VLAN+C-VLAN').

Note:

- UserVLAN: VLAN carried by upstream packets of user-side devices, U for short.
- C-VLAN: VLAN added based on the ONT/ONU port. For details, see the description of the Double-tagged VLAN S+C.
- Double-tagged VLAN S+C: C indicates the inner VLAN (C-VLAN) and S indicates the outer VLAN (S-VLAN).

Copyright © Huawei Technologies Co., Ltd.

- Double-layer VLAN S+C': C' indicates the translated inner VLAN (C'-VLAN) and S indicates the outer VLAN (SVLAN).
- Single-tagged S-VLAN: Single-tagged VLAN marked or translated by the OLT. It is generally used in a single-tagged VLAN translation scenario.
- C<->S+C': Bidirectional VLAN translation: translates the inner C-VLAN and then adds one outer S-VLAN.
- C<->S+C: Bidirectional VLAN translation: maintains the inner C-VLAN and adds one outer S-VLAN.

NOTE

- The voice service is a closed service operated by carriers. The single-tagged S-VLAN is the mainstream application and is recommended.
- When the planned VLAN is single-tagged VLAN, the S-VLANs can be allocated based on the OLT device, PON board or PON port. The S-VLANs identify services and physical locations. It is recommended that you set different voice VLANs for the OLTs connected to one voice SR to avoid an excessively large broadcast domain of the SR and convergence switch.
- When the planned VLAN is S-VLAN+C-VLAN (that is, double-tagged VLAN), the outer S-VLANs can be allocated based on the OLT device, PON board or PON port. The S-+VLANs identify services and physical locations. It is recommended to allocate S-VLANs based on PON board or PON port. The inner C-VLAN is used to identify services (a fixed value) or users.

Voice Data Plan Based on H.248 or SIP

Item			Description
MG interface/ SIP interface data **NOTE** must be consistent with the data on the MGC/IMS core network devices.	Media and signaling parameters	Media and signaling upstream VLANs	Upstream VLANs of the voice service
		Media and signaling upstream port	Upstream ports of the voice service
		Media IP addresses and signaling IP addresses	Supports separating media from signaling.
		Default gateway IP address.	The next hop IP address from an ONU/HGW to an MGC/IMS.
	MG interface/SIP interface ID		-
	Signaling port ID		Choose the transmission mode according to the requirement of the MGC/IMS side.
	IP address of active MGC (H.248)/IP address of active IMS device (SIP)		If the dual homing is not configured, only one MGC parameter needs to be configured. If the dual homing is configured, the IP address and port ID of the standby MGC need to be configured.
	Port ID of active MGC (H248)/ port ID of active IMS device (SIP)		

Copyright © Huawei Technologies Co., Ltd.

Item		Description
	Coding	Choose the coding method according to the requirement on the MGC/IMS side. Generally, the text coding method is adopted.
	Transmission mode	Choose the transmission mode according to the requirement on the MGC/IMS side. Generally, the UDP transmission mode is adopted.
	Home domain (SIP)	-
	Profile index	-
	The version of H248 protocol that MG starts to negotiate	V1, V2 or V3 (by default). The interface may fail to be registered because some softswitches do not support V3.
Voice user configuration data	Phone number	For H248 protocol: The phone numbers allocated by the MGC need to be determined, and the paging numbers for users' emergency standalone need to be planned if the emergency standalone function is provided. For SIP protocol: The phone number that the IMS core network device allocates to the user must be configured.
	Terminal ID (H248)	If the TID template with which the POTS user is bound does not support terminal layering, this parameter needs to be configured.
	User priority	According to the service requirements, user priorities must be specified. The user priorities include the following: ● cat1: government1 (category 1 government users) ● cat2: government2 (category 2 government users) ● cat3: common (common users)
	User type	According to the service requirements, user type needs to be specified. The user type includes the following: ● DEL: direct exchange lines (default) ● ECPBX: earth calling PBX ● LCPBX: loop calling PBX ● PayPhone: pay phone

Copyright © Huawei Technologies Co., Ltd.

Item		Description
Common parameter	system parameter	The system parameters including the overseas version flag and message waiting indication (MWI) mode need to be configured according to the local standard to ensure that the response of the user terminal complies with the local standard.
	Overseas parameters	The attributes such as the upper and lower thresholds of the flash-hooking duration need to be configured according to the local standards to ensure that the response of the user terminal complies with the local standards.
	POTS port attributes	If the POTS port needs to support the polarity reversal accounting, the POTS port needs to be configured to support the polarity reversal pulse. Other attributes need not be modified if there is no special requirement.
	Ringing current attributes	When the attributes of ring current are changed, ring volume is changed accordingly. Generally, no adjustment is required for the ringing tone volume. You need to modify the parameters of the ringing current attributes according to the local standard only when the default ringing current attributes do not comply with the local standard.

9.6.5 Principle of IPTV Service Data Plan

The IPTV service data plan mainly include the plan of VLAN and VLAN translation policy in different network scenario, and the plan of IPTV service.

IPTV services include multicast service and video on demand (VoD) service. These two services are relevant but independent in VLAN planning.

VLAN and VLAN Translation Policy.

Application Scenario	Service Type	VLAN Plan	VLAN Translation Policy
Bridging +Voice ONT	Multicast service	Single-tagged VLAN	ONTs replicate multicast packets based on user ports and multicast VLANs (M-VLANs) are removed downstream. The OLT replicates multicast packets based on PON ports with M-VLAN unchanged.

Copyright © Huawei Technologies Co., Ltd.

Application Scenario	Service Type	VLAN Plan	VLAN Translation Policy
	VoD	Single-tagged VLAN	ONTs add S-VLAN tags to iTV service packets. The OLT transparently transmits packets with S-VLANs.
		Double-tagged VLAN	All ONTs add the same C-VLAN tag to packets. The OLT implements VLAN translation: C->S+C'.
Bridging ONT + HGW	Multicast service	Single-tagged VLAN	ONTs transparently transmit upstream packets with M-VLANs sent from HGW. Multicast packets are replicated downstream with M-VLAN unchanged. The OLT replicates multicast packets based on PON ports with M-VLAN unchanged.
		Single-tagged VLAN	ONTs translate the upstream VLANs sent from HGW to M-VLANs. The OLT replicates multicast packets based on PON ports with M-VLAN unchanged.
	VoD	Single-tagged VLAN	ONTs transparently transmit the upstream U-VLANs sent from HGW. The OLT implements VLAN translation: U->S.
		Double-tagged VLAN	ONTs transparently transmit the upstream U-VLANs sent from HGW. The OLT implements VLAN translation: U->S+C.
Gateway ONT	Multicast service	Single-tagged VLAN	ONTs replicate packets based on user ports and M-VLANs are removed in downstream direction. The OLT replicates multicast packets based on PON ports with M-VLAN unchanged.
	VoD	Single-tagged VLAN	ONTs add C-VLAN tags to packets (iTMS system has finished the configuration). Untagged VLANs are translated to C-VLANs. The OLT implements VLAN translation: C -> S.

Note:

- UserVLAN: VLAN carried by upstream packets of user-side devices, U for short.

Copyright © Huawei Technologies Co., Ltd.

- C-VLAN: VLAN added based on the ONT/ONU port. For details, see the description of the Double-tagged VLAN S+C.
- Double-tagged VLAN S+C: C indicates the inner VLAN (C-VLAN) and S indicates the outer VLAN (S-VLAN).
- Double-layer VLAN S+C': C' indicates the translated inner VLAN (C'-VLAN) and S indicates the outer VLAN (SVLAN).
- Single-tagged S-VLAN: Single-tagged VLAN marked or translated by the OLT. It is generally used in a single-tagged VLAN translation scenario.
- C<->S+C': Bidirectional VLAN translation: translates the inner C-VLAN and then adds one outer S-VLAN.
- C<->S+C: Bidirectional VLAN translation: maintains the inner C-VLAN and adds one outer S-VLAN.

NOTE

- IPTV service is a closed service self-operated by carriers, and single-tagged S-VLAN is recommended.
- The same S-VLAN or different S-VLANs can be used as the M-VLAN and VoD VLAN. It is recommended that you use different S-VLANs as M-VLAN and VoD VLAN so that the upper-level device easily differentiates between the BTV service and VoD service.
- S-VLANs of VoD service can identify services and physical locations based on an entire network or an OLT. It is recommended that you set different VoIP VLANs for the OLTs connected to one VoIP SR to avoid an excessively large broadcast domain of the VoIP SR and convergence switch.

9.6.6 Principle of Security Data Plan

The security plan involves system security plan, user security plan, and service security plan. Security policy ensures service security from different aspects.

NOTE

The device provides complete security measures, but not all security measures need to be deployed. Only the security measures that meet the following requirements need to be deployed:

- The security measures can be used on the live network.
- The security measures are easy to deploy.
- The security measures are effective.

System Security

Security Vulnerability	Solution	Description and Usage Suggestion
DoS attack	Enable the anti-DoS-attack function for OLT.	After the anti-DoS-attack function is enabled, control packets are monitored and those exceeding the number threshold are discarded. Use this solution for new site deployment.

Copyright © Huawei Technologies Co., Ltd.

Security Vulnerability	Solution	Description and Usage Suggestion
IP attack	Enable the anti-IP-attack function for OLT.	After the anti-IP-attack function is enabled, a device discards the IP packets received from the user side whose destination IP address is the IP address of the device, and therefore the system is protected. Use this solution for new site deployment.

User Security

Security Vulnerability	Solution	Description and Usage Suggestion
MAC spoofing	Enable the anti-MAC-duplicate function for OLT.	After anti-MAC-duplicate is enabled, the system records the first MAC address learnt from the port and binds the MAC address to the port and VLAN. If receiving packets sent from the host that has the same MAC address with the port, the system discards the packets directly. In this case, it can prevent users from forging MAC addresses to perform malicious attacks. Use this solution for new site deployment.
MAC attack	Enable the anti-MAC spoofing function for OLT.	After anti-MAC spoofing is enabled, the system can prevent users from forging MAC addresses to perform malicious attacks. Use this solution for new site deployment.
IP spoofing	Enable the anti-IP spoofing function for OLT.	After anti-IP spoofing is enabled, the system can prevent users from forging IP addresses to perform malicious attacks. Use this solution for new site deployment.

Copyright © Huawei Technologies Co., Ltd.

Service Security

Security Vulnerability	Solution	Description and Usage Suggestion
Unauthorized broadband access of small enterprises (IPoE)	DHCP option 82 is enabled on OLT, and the BRAS implements user authentication based on the RAIO information.	In the DHCP option 82 mode, user's physical location is added to the option 82 field carried in the DHCP request packet initiated by a user. The physical location, used for user authentication on the upper-layer authentication server, can help implement the following functions: ● The DHCP relay forwards DHCP response packets to devices with specified CID and RID. ● Prevents DHCP address exhaustion. ● Achieves static allocation of DHCP addresses. ● Implements anti-IP spoofing. ● Implements anti-user ID spoofing. ● Implements anti-MAC spoofing. Use this solution for the DHCP Internet access service.
Broadband access of residential users (PPPoE), user account theft/ borrowing	PPPoE+ (PITP) is enabled on OLT, and the BRAS implements user authentication based on binding of the RAIO information to the user account.	The BRAS responds to request packets of users with specified CID and RID. In this way, the following functions are implemented: ● Prevents IP address exhaustion. ● Implements anti-IP spoofing. ● Implements anti-user ID spoofing. ● Implements anti-MAC spoofing. Use this solution for the PPPoE Internet access service.

9.7 GPON Access: Configuring FTTH Service

This topic describes how to configure the Internet access service, voice service and BTV service and VoD service in GPON access mode in FTTH network scenario.

Context

There are two xPON configuration modes: distributed mode (also called discrete mode) and profile mode. The difference between the two modes lies in command lines.

Copyright © Huawei Technologies Co., Ltd.

- Distributed mode: In this mode, ONTs need to be configured one by one but not in batches.
- Profile mode: In this mode, an ONT line profile and service profile are configured first. Then, ONTs can be added in batches by binding profiles. This mode greatly improves service provisioning efficiency.

Generally, the xPON configuration mode is determined in a new deployment and will not be changed. This chapter describes how to configure the enterprise access service in PON profile mode (which is the default mode). You can run the commands in the following table to query the xPON configuration mode.

Mode	Query Method
PON profile mode	huawei(config)#**diagnose** huawei(diagnose)%%**display xpon mode** -- Current config mode: Profile-mode --

NOTE

For commands for the distributed configuration mode, see **PON distributed-mode commands** in the *Command Reference*.

9.7.1 Bridging+Voice ONT Network Scenario

This topic describes how to configure Internet access service, voice service, BTV service and VoD service when bridging+voice ONTs are used to build an FTTH network.

9.7.1.1 Service Requirements and Application Scenario

Service Requirements

Optical fibers are connected to user homes and triple play services are required. The following provides detailed service requirements:

- Internet access of multiple PCs in a home is supported.
- Access of multiple telephones in a home is supported.
- IPTV programs can be previewed and watched using STBs.
- Service extension is supported and different services do not affect each other.
- Proper service security is ensured.
  - Internet access services are protected against unauthorized access, user account theft or borrowing, MAC/IP spoofing, and malicious attacks.
  - Voice and IPTV services are protected against MAC/IP spoofing, malicious attack, and traffic flooding attacks.
- Service faults are easy to locate and services are easy to maintain.

Application Scenario

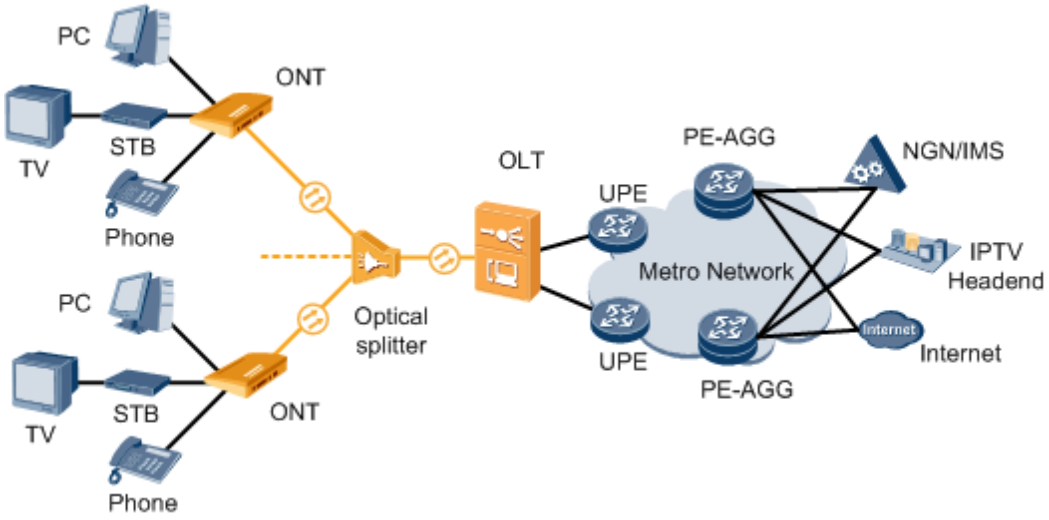
As shown in **Figure 9-1**, the ONT integrating an integrated access device (IAD) provides Internet, VoIP, and IPTV services to users.

Copyright © Huawei Technologies Co., Ltd.

The bridging+voice ONT provides Layer 2 data (Internet and IPTV services) and VoIP services. This scenario provides transparent transmission channels and requires simple service configuration, so this scenario applies to Layer 2 networking.

- For Internet services, a PC directly performs dial-up. Then, the upper-layer broadband remote access server (BRAS) device authenticates and accesses the PC. The PC can also access the Internet using the Dynamic Host Configuration Protocol (DHCP) or static IP address.
- For VoIP services, the ONT with a bulit-in voice module encapsulates voice service packets, and the OLT transmits them to the upstream next generation network (NGN) or IP multimedia subsystem (IMS).
- For IPTV services, the set top box (STB) obtains an IP address from the DHCP server for ordering programs. The ONT transparently transmits the packets.

Figure 9-1 Bridging+Voice ONT

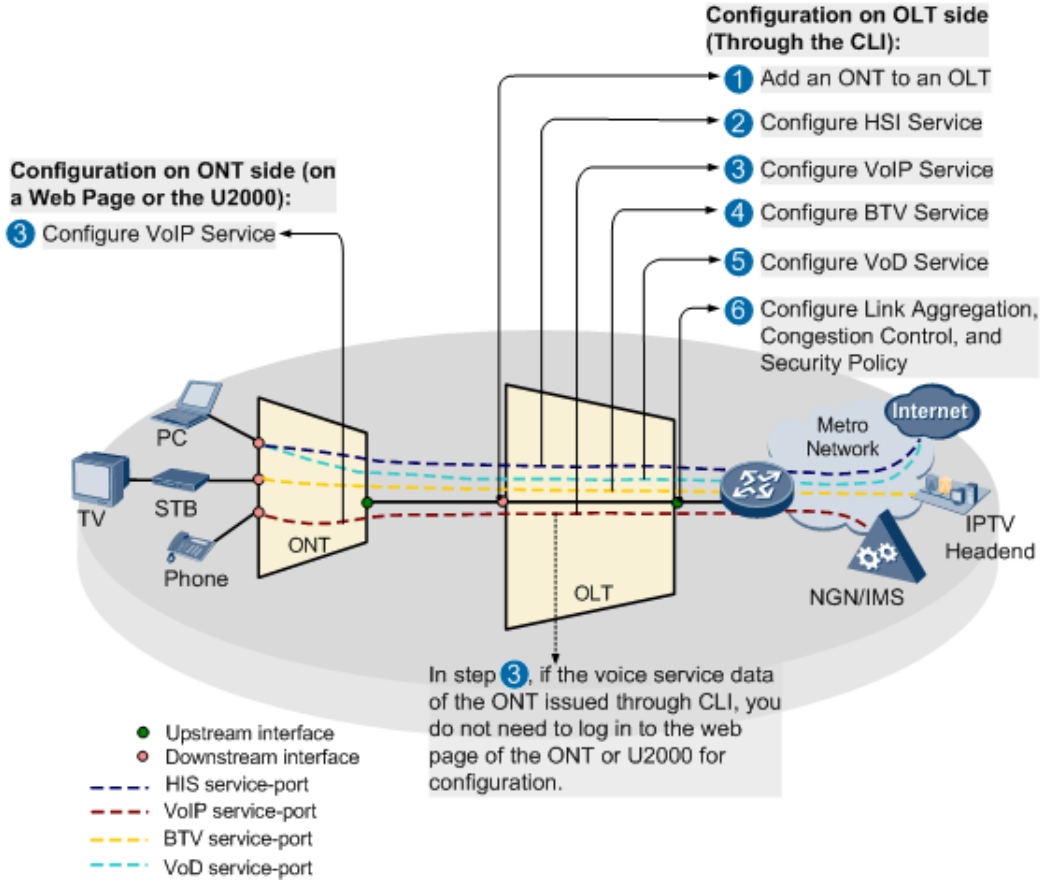


9.7.1.2 Configuration Process

Figure 9-2 shows the configuration roadmap in fiber to the home (FTTH) networking using a bridging+voice optical network terminal (ONT).

Copyright © Huawei Technologies Co., Ltd.

Figure 9-2 Configuration roadmap in FTTH networking using a bridging+voice ONT



The following table describes the configuration steps.

Item	Step	Description
Optical line terminal (OLT)	**9.7.1.3 Adding an ONT to an OLT**	Services can be configured for an ONT only after the ONT is successfully added to an OLT.
OLT	**9.7.1.4 Configuring the Internet Access Service**	None

Copyright © Huawei Technologies Co., Ltd.

Item	Step		Description

OLT
ONT
U2000
	Configure the VoIP service.	**9.7.1.5 Configuring the H.248-based Voice Service (on a Web Page or the U2000)**	**NOTE**
			● The H.248 and Session Initiation Protocol (SIP) protocols are mutually exclusive for the VoIP service. Either of them is configured at a time.
			● The voice service can be configured through command line interface (CLI) on an OLT, web page, or U2000. Select a configuration mode based on site requirements.
			  ● OLT CLI: This mode can be used for site deployment or the U2000 has not been deployed.
			  ● Web page: This mode can be used to configure voice parameters after the service channel has been configured through the OLT CLI. It can be used for site deployment.
			  ● U2000: This mode can be used to configure voice parameters after the service channel has been configured through the OLT CLI. It can be used for service provisioning in batches.

		9.7.1.6 Configuring the H.248-based Voice Service (Through the CLI)	
		9.7.1.7 Configuring the SIP-based Voice Service (on a Web Page or the U2000)	
		9.7.1.8 Configuring the SIP-based Voice Service (Through the CLI)	
OLT	Configure the IPTV service.	**9.7.1.9 Configuring the BTV Service**	IPTV services include the BTV and VoD services that are different in configuration procedures and need to be configured separately.
		9.7.1.10 Configuring the VoD Service	
OLT	**9.7.1.11 Configuring Link Aggregation, Congestion Control, and Security Policies**		The global configuration of link aggregation and queue scheduling based on priorities ensures service reliability. The global configuration of security policies ensures service security.

Copyright © Huawei Technologies Co., Ltd.

Item	Step	Description
OLT	9.7.1.12 Verifying Services	The OLT provides remote verification methods including ONT PPPoE/DHCP dialup emulation and call emulation for configuration and commissioning engineers to verify services remotely after service configuration, avoiding a second on-site operation.

9.7.1.3 Adding an ONT to an OLT

Services can be configured for an ONT only after the ONT is successfully added to an OLT.

Data Plan

Table 9-2 Data plan

Item	Data
DBA profile	Profile name: ftth_dba Profile type: type3 Assured bandwidth: 8 Mbit/s Maximum bandwidth: 20 Mbit/s
ONT line profile	Profile name: ftth T-CONT ID: 4 GEM port ID for management services: 11 GEM port ID for voice services: 12 GEM port ID for video services: 13 GEM port ID for Internet access services: 14
ONT service profile	Profile name: ftth ONT port capability set: adaptive
Network topology data	PON port: 0/1/0 ONT IDs: 1 and 2

Procedure

Step 1 Configure GPON ONT profiles.

GPON ONT profiles include the DBA profile, line profile, service profile, and alarm profile.

- DBA profile: A DBA profile describes GPON traffic parameters. A T-CONT is bound to a DBA profile for dynamic bandwidth allocation, improving upstream bandwidth utilization.

Copyright © Huawei Technologies Co., Ltd.

- Line profile: A line profile describes the binding between the T-CONT and the DBA profile, the QoS mode of the traffic stream, and the mapping between the GEM port and the ONT-side service.
- Service profile: A service profile provides the service configuration channel for the ONT that is managed by using optical network terminal management and control interface (OMCI).
- Alarm profile: An alarm profile contains a series of alarm thresholds to measure and monitor the performance of activated ONT lines. When a statistical value reaches the threshold, the host is notified and an alarm is reported to the log host and the NMS.

1. Configure a DBA profile.

   Run the **display dba-profile** command to query existing DBA profiles in the system. If the existing DBA profiles in the system do not meet the requirements, run the **dba-profile add** command to add a DBA profile.

   Create the same DBA profile for different types of services. Set the profile name to **ftth_dba**, profile type to **type3**, assured bandwidth to 8 Mbit/s, and maximum bandwidth to 20 Mbit/s.

   ```
   huawei(config)#dba-profile add profile-name ftth_dba type3 assure 8192 max
   20480
   ```

   NOTE

   The DBA implementation is based on an ONT. Therefore, select a DBA profile of the proper bandwidth type and configure proper bandwidth according to the service types and total user count of the ONT. Note that the sum of the fixed bandwidth and the assured bandwidth must not be greater than the total bandwidth of the PON port.

2. Configure an ONT line profile.

   Create a GPON ONT line profile, named **ftth**, and bind it to the DBA profile **ftth_dba**.

   ```
   huawei(config)#ont-lineprofile gpon profile-name ftth
   huawei(config-gpon-lineprofile-1)#tcont 4 dba-profile-name ftth_dba
   ```

   Create different GEM ports according to different service types, in which

   - GEM port 11 is used to carry management services.
   - GEM port 12 is used to carry voice services.
   - GEM port 13 is used to carry video services.
   - GEM port 14 is used to carry Internet access services.

   ```
   huawei(config-gpon-lineprofile-1)#gem add 11 eth tcont 4
   huawei(config-gpon-lineprofile-1)#gem add 12 eth tcont 4
   huawei(config-gpon-lineprofile-1)#gem add 13 eth tcont 4
   huawei(config-gpon-lineprofile-1)#gem add 14 eth tcont 4
   ```

   NOTE

   1. To change the default QoS mode, run the **qos-mode** command to set the QoS mode to **gem-car** or **flow-car**, and run the **gem add** command to set the index of the traffic profile bound to the GEM port.
   2. When the QoS mode is priority-queue (PQ), the default queue priority is 0; when the QoS mode is flow-car or gem-car, traffic profile 6 is bound to the GEM port by default (no rate limitation).

   After the configurations are complete, run the **commit** command to apply the parameters settings.

   ```
   huawei(config-gpon-lineprofile-1)#commit
   huawei(config-gpon-lineprofile-1)#quit
   ```

3. Configure an ONT service profile.

Copyright © Huawei Technologies Co., Ltd.

Create a GPON ONT service profile, named **ftth**. Configure the capability set of the ETH port and POTS port to **adaptive**. Then the system automatically adapts to the ONT according to the actual capability of the online ONT.

```
huawei(config)#ont-srvprofile gpon profile-name ftth
huawei(config-gpon-srvprofile-1)#ont-port eth adaptive pots adaptive
```

After the configurations are complete, run the **commit** command to apply the parameters setting.

```
huawei(config-gpon-srvprofile-1)#commit
huawei(config-gpon-srvprofile-1)#quit
```

4. (Optional) Add an alarm profile.
   - The default GPON alarm profile 1 is used. The alarm thresholds of the default alarm profile are 0, which indicates that no alarm is generated.
   - In this example, the default alarm profile is used, and therefore the configuration of the alarm profile is not required.
   - Run the **gpon alarm-profile add** command to configure a GPON alarm profile, which is used for monitoring the performance of an activated ONT line.

Step 2 Add an ONT.

Connect two ONTs to GPON port 0/1/0. Set the ONT IDs to **1** and **2**, SNs to **32303131D659FD40** and **6877687714852901**, passwords to **0100000001** and **0100000002**, discovery mode for password authentication to **once-on**, and management mode to **OMCI**. Bind the two ONTs to ONT line profile **ftth** and ONT service profile **ftth**.

There are two methods of adding an ONT: add an ONT offline and confirm an automatically discovered ONT.

- Add ONTs offline.

  If the password of an ONT is known, run the **ont add** command to add an ONT offline.

```
huawei(config)#interface gpon 0/1
huawei(config-if-gpon-0/1)#ont add 0 1 password-auth 0100000001 once-on no-aging
omci ont-lineprofile-name
 ftth ont-srvprofile-name ftth
huawei(config-if-gpon-0/1)#ont add 0 2 password-auth 0100000002 once-on no-aging
omci ont-lineprofile-name
 ftth ont-srvprofile-name ftth
```

- Confirm automatically discovered ONTs.

  If the password or SN of an ONT is unknown, run the **port** *portid* **ont-auto-find** command in GPON mode to enable the ONT auto-discovery function of the GPON port. Then, run the **ont confirm** command to confirm the ONT.

```
huawei(config)#interface gpon 0/1
huawei(config-if-gpon-0/1)#port 0 ont-auto-find enable
huawei(config-if-gpon-0/1)#display ont autofind 0
  //After this command is executed, the information about all ONTs connected to
the GPON port through optical splitters is displayed.

huawei(config-if-gpon-0/1)#ont confirm 0 ontid 1 sn-auth 32303131D659FD40 omci
ont-lineprofile-name
 ftth ont-srvprofile-name ftth
huawei(config-if-gpon-0/1)#ont confirm 0 ontid 2 sn-auth 6877687714852901 omci
ont-lineprofile-name
 ftth ont-srvprofile-name ftth
```


Copyright © Huawei Technologies Co., Ltd.

NOTE

If multiple ONTs of the same type bound to the same line profile or service profile are connected to the same port, you can bulk add ONTs by bulk confirming automatically discovered ONTs to make configuration easier and more efficient. To do so, the preceding command can be modified as follows:

```
huawei(config-if-gpon-0/1)#ont confirm 0 all sn-auth omci ont-lineprofile-name
ftth
ont-srvprofile-name ftth
```

- (Optional) Bind the alarm profile to the ONT.

  The default profile 1 is used in this example.

```
huawei(config-if-gpon-0/1)#ont alarm-profile 0 1 profile-id 1
huawei(config-if-gpon-0/1)#ont alarm-profile 0 2 profile-id 1
```

Step 3 Check ONT status.

After an ONT is added, run the **display ont info** command to query the current status of the ONT. Ensure that **Config flag** of the ONT is **active**, **Run State** is **online**, **Config state** is **normal**, and **Match state** is **match**.

```
huawei(config-if-gpon-0/1)#display ont info 0 1
  ------------------------------------------------------------------------
  F/S/P                : 0/1/0
  ONT-ID               : 1
  Control flag         : active    //Indicates that the ONT is
activated.
  Run state            : online    //Indicates that the ONT goes online
successfully.
  Config state         : normal    //Indicates that the configuration state of the
ONT is normal.
  Match state          : match     //Indicates that the capability profile bound to
the ONT is consistent with the actual capability of the ONT.
...//The rest of the response information is omitted.
```

When **Config state** is **failed**, **Run state** is **offline**, or **Match state** is **mismatch**:

- If **Control flag** is **deactive**, run the **ont active** command in GPON mode to activate the ONU.
- If **Run state** is **offline**, a physical line may be broken or the optical module may be damaged. Check the line and the optical module.
- If **Config state** is **failed**, the configured ONU capability exceeds the actual ONU capability. In this case, run the **display ont failed-configuration** command in the diagnose mode to check the failed configuration item and the failure cause. Then, rectify the fault accordingly.
- If the ONU does not match, that is, **Match state** is **mismatch**, the port types and number of ports undermatch the actual port types and number of ports supported by the ONU. In this case, run the **display ont capability** command to query the actual capability of the ONU, and then select one of the following modes to modify the ONU configuration:
  - Create a proper ONU profile according to the actual capability of the ONU, and then run the **ont modify** command to modify the configuration data of the ONU.
  - Modify the ONU profile according to the actual capability of the ONU and save the modification. Then, the ONU automatically recovers the configuration successfully.

----End

9.7.1.4 Configuring the Internet Access Service

The OLT is connected to the remote ONT through a GPON port to provide users with high-speed Internet access services.

Copyright © Huawei Technologies Co., Ltd.

Prerequisites

- The OLT is connected to the BRAS.
- Related configurations are performed on the BRAS according to the authentication and accounting requirements for dialup users. For details about the configuration, see the configuration guide.
- The ONT has been added to the OLT. For details, see **9.7.1.3 Adding an ONT to an OLT**.
- The VLAN of the LAN switch port connected to the OLT is consistent with the upstream VLAN of the OLT.

Data Plan

Item	Data
ONT line profile	Profile name: ftth T-CONT ID: 4 GEM port ID for Internet access service: 14
Network topology data	Upstream port: 0/19/0 PON port: 0/1/0 ONT IDs: 1 and 2 ID of the port on the ONT that is connected to the PC: 1
VLAN Plan	Double-tagged VLAN: ● S-VLAN ID: 100 ● S-VLAN type: smart ● S-VLAN attribute: stacking ● CVLAN ID: 1001 ● C'-VLAN ID: 1010-1011 VLAN Translation Policy: ● ONT: ONTs configure the VLAN and add the same C-VLAN tag to packets. All ONTs are in the same C-VLAN. ● OLT: The OLT performs VLAN translation: C<->S+C'. The C'-VLAN of every ONT differs from each other.

Procedure

- Configure the OLT.
  1. Configure a traffic profile.

     Run the **display traffic table ip** command to query existing traffic profiles in the system. If the traffic profiles existing in the system do not meet the requirements, you need to run the **traffic table ip** command to add a traffic profile.

Copyright © Huawei Technologies Co., Ltd.

Set the profile ID to ftth_hsi, the CIR to 4 Mbit/s, and the priority to 0. In addition, configure the scheduling mode so that packets are scheduled according to their priorities.

```
huawei(config)#traffic table ip name ftth_hsi cir 4096 priority 0 priority-policy local-setting
```

2. Configure the mapping between a GEM port and a VLAN.

   The service flow of C-VLAN 1001 is mapped to GEM port 14 in the ONT line profile.

```
huawei(config)#ont-lineprofile gpon profile-name ftth
huawei(config-gpon-lineprofile-1)#gem mapping 14 0 vlan 1001
huawei(config-gpon-lineprofile-1)#commit
huawei(config-gpon-lineprofile-1)#quit
```

3. Configure the VLAN of the Ethernet port on the ONT.

   If the ONT is connected to the PC through Ethernet port 1, add Ethernet port 1 to VLAN 1001 in the ONT service profile.

```
huawei(config)#ont-srvprofile gpon profile-name ftth
huawei(config-gpon-srvprofile-1)#port vlan eth 1 1001
huawei(config-gpon-srvprofile-1)#commit
huawei(config-gpon-srvprofile-1)#quit
```

4. Configure the native VLAN of the ONT port.

   Set the native VLAN ID of Ethernet port 1 to 1001.

```
huawei(config)#interface gpon 0/1
huawei(config-if-gpon-0/1)#ont port native-vlan 0 1 eth 1 vlan 1001
huawei(config-if-gpon-0/1)#ont port native-vlan 0 2 eth 1 vlan 1001
huawei(config-if-gpon-0/1)#quit
```

5. Create an Internet access service VLAN and add an upstream port to it.

   Add upstream port 0/19/0 to VLAN 100.

```
huawei(config)#vlan 100 smart
huawei(config)#vlan attrib 100 stacking
huawei(config)#port vlan 100 0/19 0
```

6. Create service flows.

   Set the service VLAN to 100, GEM port ID to 14, and user VLAN to 1001. Use traffic profile ftth_hsi.

```
huawei(config)#service-port vlan 100 gpon 0/1/0 ont 1 gemport 14 multi-service
user-vlan 1001 tag-transform translate-and-add inner-vlan 1010 inbound traffic-table name
ftth_hsi outbound traffic-table name ftth_hsi
huawei(config)#service-port vlan 100 gpon 0/1/0 ont 2 gemport 14 multi-service
user-vlan 1001 tag-transform translate-and-add inner-vlan 1011 inbound traffic-table name
ftth_hsi outbound traffic-table name ftth_hsi
```

7. Save the data.

```
huawei(config)#save
```

- The ONT does not need to be configured.

----End

Copyright © Huawei Technologies Co., Ltd.

9.7.1.5 Configuring the H.248-based Voice Service (on a Web Page or the U2000)

The OLT is connected to the remote ONT through a GPON port to provide users with the IP-based high-quality and low-cost VoIP service.

Prerequisites

- The interface data and POTS user configuration data corresponding to the MG interface have been configured on the MGC.
- The OLT has been connected to the MGC. The OLT can ping the IP address of the MGC server successfully.
- The ONT has been added to the OLT. For details, see **9.7.1.3 Adding an ONT to an OLT**.
- Different voice services require different ONT software versions. Before the configuration, ensure that the current ONT software version supports H.248. For details, see relevant ONT manuals.

Data Plan

Item	Data
ONT line profile	Profile name: ftth T-CONT ID: 4 GEM port ID: 12
VLAN plan	Single VLAN tag: ● VLAN ID: 300 ● VLAN type: smart ● VLAN attribute: common ● CVLAN=SVLAN VLAN translation policy: ● ONT: VLANs are configured for the ONTs on the same network in a unified manner, and the ONTs have the same C-VLAN. The ONT adds a C-VLAN tag to packets. ● OLT: transparently transmits the VLAN.
Voice parameter	IP address of the MGC server: 200.200.200.200/24 Port ID of the MGC server: 2944 MG Domain: 0100000001 or 0100000002

Procedure

- Configure the OLT.
  1. Configure a traffic profile.

Copyright © Huawei Technologies Co., Ltd.

Run the **display traffic table ip** command to query the existing traffic profiles in the system. If the existing traffic profiles in the system do not meet the requirements, run the **traffic table ip** command to add a traffic profile.

Set the profile name to **ftth_voip** and do not limit the upstream and downstream rates. Set the priority to **5** and packets are scheduled according to the priority carried.

```
huawei(config)#traffic table ip name ftth_voip cir off priority 5 priority-
policy
 local-setting
```

2. Configure the mapping relationship between a GEM port and a VLAN.

   The service flow of user VLAN 300 is mapped to GEM port 12 in the ONT line profile.

   ```
   huawei(config)#ont-lineprofile gpon profile-name ftth
   huawei(config-gpon-lineprofile-1)#gem mapping 12 2 vlan 300
   huawei(config-gpon-lineprofile-1)#commit
   huawei(config-gpon-lineprofile-1)#quit
   ```

3. Create a service VLAN and add an upstream port to it.

   Add upstream port 0/19/0 to VLAN 300.

   ```
   huawei(config)#vlan 300 smart
   huawei(config)#port vlan 300 0/19 0
   ```

4. Create service flows.

   Set the service VLAN to 300, GEM port ID to 12, and user VLAN to 300, and use traffic profile **ftth_voip**.

   ```
   huawei(config)#service-port vlan 300 gpon 0/1/0 ont 1 gemport 12 multi-
   service
    user-vlan 300 inbound traffic-table name ftth_voip outbound traffic-table
   name
   ftth_voip
   huawei(config)#service-port vlan 300 gpon 0/1/0 ont 2 gemport 12 multi-
   service
    user-vlan 300 inbound traffic-table name ftth_voip outbound traffic-table
   name
   ftth_voip
   ```

5. Enable the ARP proxy function.

   Voice media streams for different users of the same SVLAN fail to interchange because the service ports of the smart VLAN are isolated from each other. Therefore, the ARP proxy function needs to be enabled on the OLT.

   ```
   huawei(config)#arp proxy enable
   huawei(config)#interface vlanif 300
   huawei(config-if-vlanif300)#arp proxy enable
   huawei(config-if-vlanif300)#quit
   ```

6. Save the data.

   ```
   huawei(config)#save
   ```

- Configure the ONT on the Web page.

  Log in to the Web page and then configure the ONT on the Web page.

  1. Configure the IP address of the PC network adapter to be in the same network segment with the IP address of the local maintenance Ethernet port on the ONT (default: 192.168.100.1).
  2. Open the Web browser, and enter the IP address (https://192.168.100.1:80 or http://192.168.100.1) (https with high priority is recommended) of the local maintenance Ethernet port on the ONT. In the login window that is displayed, enter the user name

Copyright © Huawei Technologies Co., Ltd.

(default telecomadmin) and password (default admintelecom) of the administrator. After the password is authenticated, the web configuration window is displayed.

NOTE

- The following configuration procedure is for scenarios with the bridging ONT. For scenarios with the bridging ONT+HGW, configure the voice service on the HGW but not on the ONT. For detailed configurations, see the HGW Configuration Guide.
- The Web page for configuring ONT varies with ONT versions, but the parameter configuration is the same. For details, see relevant ONT manuals.

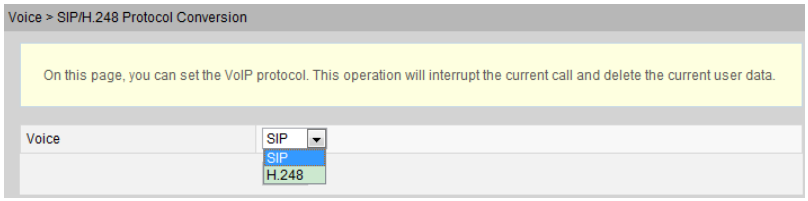
1. Configure the voice protocol.

   NOTE

   The default voice protocol is SIP. Therefore, change the voice protocol first.

   a. Choose **Voice** > **SIP/H.248 Protocol Conversion**.

   b. In the pane on the right, set **Voice** to **H.248**.

   c. Click **Apply**.

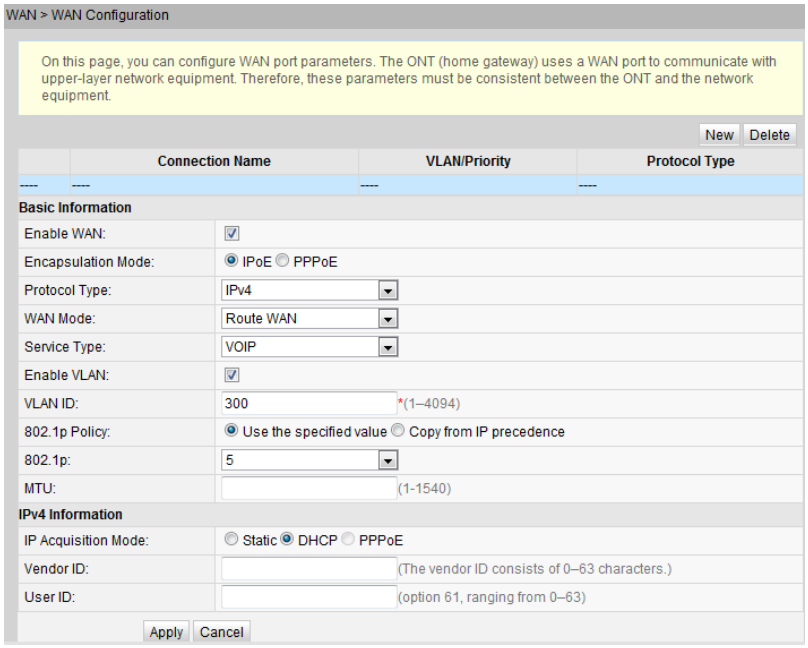
2. Configure parameters for the voice WAN interface.

   a. Choose **WAN** > **WAN Configuration**.

   b. In the right pane, click **New**. In the dialog box that is displayed, set the parameters as follows:

      - Select **Enable WAN Connection** to enable the new WAN connection.
      - Set **Encapsulation mode** to **IPoE**.
      - Set **Service Type** to **VOIP**. (For configuring the VoIP service, VoIP or a combination containing VoIP needs to be selected.)
      - Set **WAN mode** to **Route WAN**.
      - Select **Enable VLAN**.
      - Set **VLAN ID** to **300**. (The VLAN ID of the ONT must be the same as the user-side VLAN ID configured on the OLT.)
      - Set **802.1p** to **5**.
      - Set **IP Acquisition Mode** to **DHCP**.

Copyright © Huawei Technologies Co., Ltd.



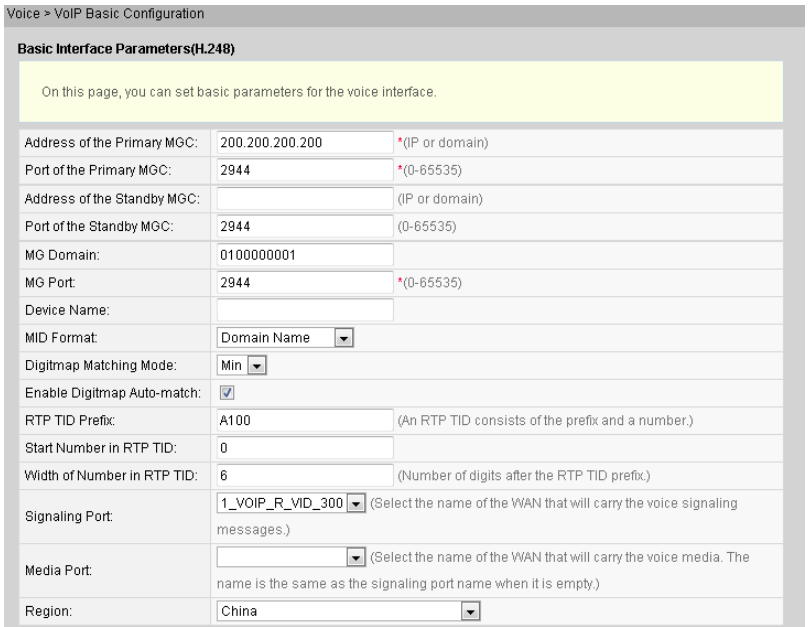
c. Click **Apply**.

3. Configure parameters for the H.248-based voice interface.

a. Choose **Voice** > **VoIP Basic Configuration**.

b. In the **Basic Interface Parameters(H.248)** window, configure the parameters as follows:

- Set **Address of the Primary MGC** to **200.200.200.200**.
- Set **MID Format** to **Domain Name** and **MG Domain** to **0100000001**.
- Set **Signaling Port** to **1_VOIP_R_VID_300**.
- Set **Region** to **China**.



Copyright © Huawei Technologies Co., Ltd.

NOTE

- The parameters of the H.248-based voice interface must be consistent with the corresponding configuration on the media gateway controller (MGC).
- If dual-homing is configured, **Address of the Standby MGC** must be configured.
- **MID Format** can be set to **Domain Name**, **IP**, or **Device Name**. If **MID Format** is set to **Domain Name** or **Device Name**, the setting must be consistent with the corresponding configuration on the MGC.
- **MG Domain** is ONT's domain name registered with the MGC. It is globally unique. **MG Domain** in this example is ONT's password.
- If **Media Port** is empty, the parameter value is the same as **Signaling Port**. The media streams are not isolated from signaling streams. If the upper-layer network requires isolation of media streams from signaling streams, create different traffic streams for the media streams and signaling streams on the OLT, create different WAN ports on the ONT, and bind the created WAN ports to **Media Port** and **Signaling Port**. When the packet is forwarded from two WAN ports, the configured VLAN is carried by default.
- When the ONT is interconnected with a third-party softswitch, check **RTP TID Prefix**, **Start Number of RTP TID**, and **Width of RTP TID Number**.

c. Configure parameters for H.248-based voice users.

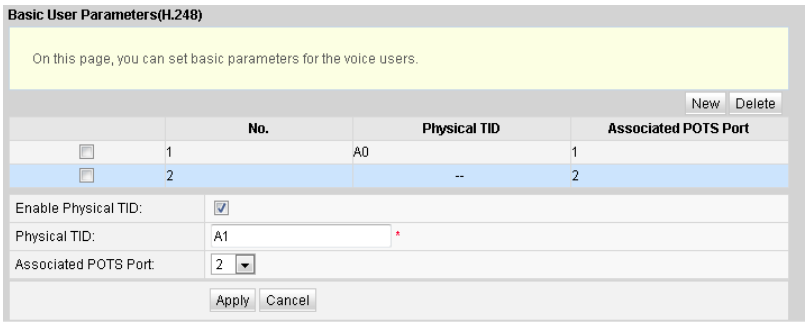
a. Choose **Voice** > **VoIP Basic Configuration**.

b. In the **Basic User Parameters(H.248)** window, set the parameters for user 1 as follows:

- Select **Enable Physical TID**.
- Set **Physical TID** to **A0**.
- Set **Associated POTS Port** to **1**.
- Click **Apply**.

Click **New** to add voice user 2, and set the parameters for voice user 2 as follows:

- Select **Enable Physical TID**.
- Set **Physical TID** to **A1**.
- Set **Associated POTS Port** to **2**.
- Click **Apply**.



NOTE

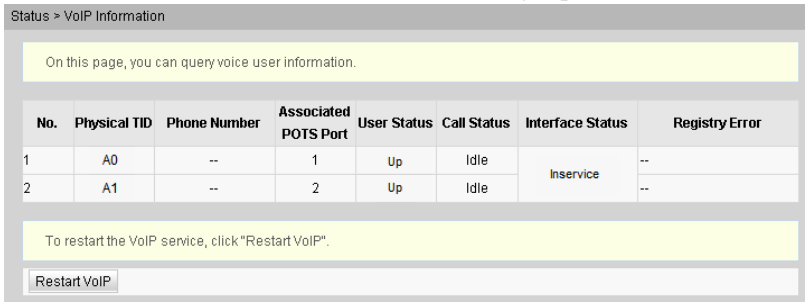
- The terminal IDs **A0** and **A1** must be consistent with the corresponding configuration on the MGC.
- If **Associated POTS Port** is **1**, port TEL1 on the ONT is bound. If **Associated POTS Port** is **2**, port TEL2 on the ONT is bound.

d. Click **Apply**.

Copyright © Huawei Technologies Co., Ltd.

4. Check the registration status of the voice user.

   Choose **Status** > **VoIP Information**. In the right pane, **User Status** is **Up**.



- Configure the ONT on the U2000.

  NOTE

  - The following configuration procedure is for scenarios with the bridging ONT. For scenarios with the bridging ONT+HGW, configure the voice service on the HGW but not on the ONT. For detailed configurations, see the HGW Configuration Guide.
  - The window for configuring ONT value-added service (VAS) profiles varies with ONT versions, but the parameter configuration is the same. For details, see relevant ONT manuals.

  1. **Configure a general VAS profile for the ONT.**

     a. From the main menu, choose **Configuration** > **Access Profile Management**. In the navigation tree of the tab page that is displayed, choose **PON Profile** > **ONT VAS Profile**.

     b. On the **General ONT VAS Profile** tab page, right-click, and choose **Add** from the shortcut menu.

     c. In the dialog box that is displayed, set **Name** to **ONT-VoIP**.

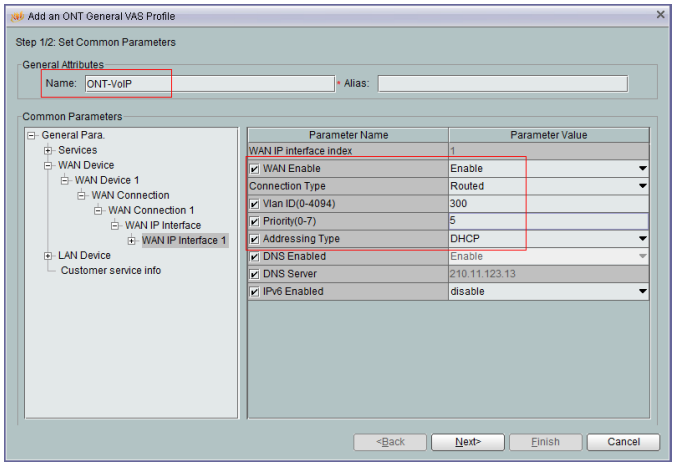
     d. Configure the parameters of a voice WAN port.

        a. In the navigation tree, choose **General Para** > **WAN Device** > **WAN Device 1** > **WAN Connection**. Select **WAN Connection**, right-click, and choose **Add IP Connection** from the shortcut menu.

        b. Select **WAN IP Interface 1** and enter (or select) a proper value.

        - WAN Enable: enable
        - Connection Type: Routed
        - VLAN ID: 300 (The VLAN ID of the ONT must be the same as the user-side VLAN ID configured on the OLT.)
        - Priority: 5
        - Addressing Type: DHCP

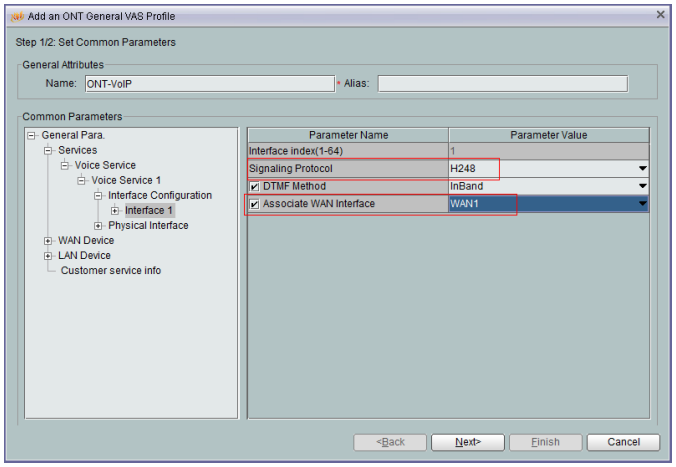
Copyright © Huawei Technologies Co., Ltd.



e. Configure parameters of the voice protocol.

In the navigation tree, choose **General Para** > **Services** > **Voice Service** > **Voice Service 1** > **Interface configuration** > **Interface 1**. Select **Interface 1** and select a proper value.

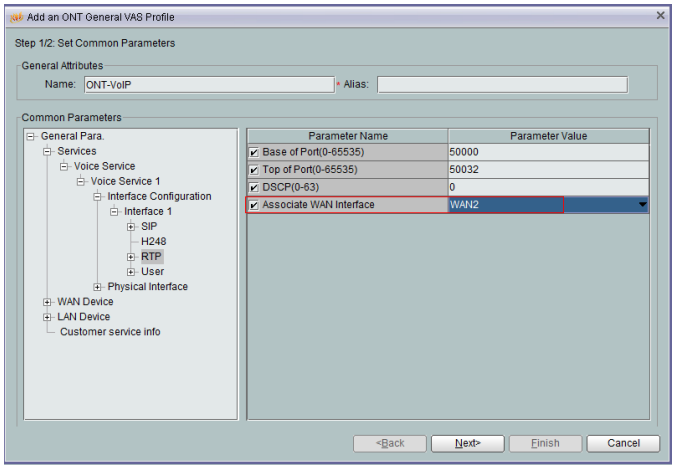
- Signaling Protocol: H.248
- Associate WAN Interface: WAN1 (binding the created voice WAN port)



NOTE

If the upper-layer network requires isolation of media streams from signaling streams, create different traffic streams for the media streams and signaling streams on the OLT. When the packet is forwarded from two WAN ports, the configured VLAN is carried by default. Create a WAN port named **WAN-RTP** on the ONT, and set this WAN port to a media WAN port. Specifically, choose **Interface 1** > **RTP** and set **Associate WAN Interface** to **WAN2**.

Copyright © Huawei Technologies Co., Ltd.



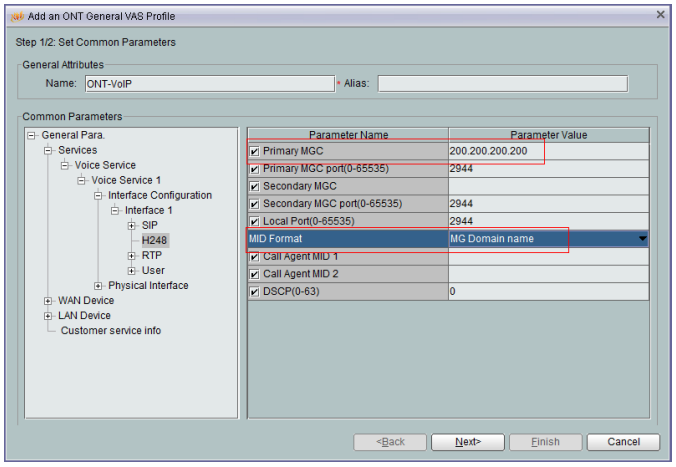
f. Configure the MGC parameters.

In the navigation tree, choose **General Para** > **Services** > **Voice Service** > **Voice Service 1** > **Interface configuration** > **Interface 1** > **H248**. Select **H248** and enter (or select) a proper value.

- Primary MGC: 200.200.200.200
- MID Format: MG Domain name

NOTE

- If dual-homing is configured, **Secondary MGC** must be set.
- **MID Format** can be set to **MG Domain Name**, **IP**, or **Device name**.



g. Configure the voice users.

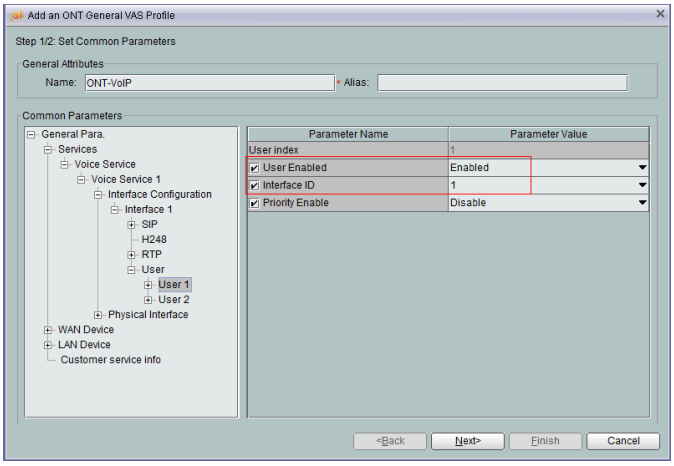
a. In the navigation tree, choose **General Para** > **Services** > **Voice Service** > **Voice Service 1** > **Interface configuration** > **Interface 1** > **User**. Right-click **User** and choose **Add** from the shortcut menu.

b. Select **User 1** under the **User** node. In the right pane, set **User Enabled** to **Enable**, and **Interface ID** to **1**. Then, select **User 2** under the **User** node. In the right pane, set **User Enabled** to **Enable**, and **Interface ID** to **2**.

NOTE

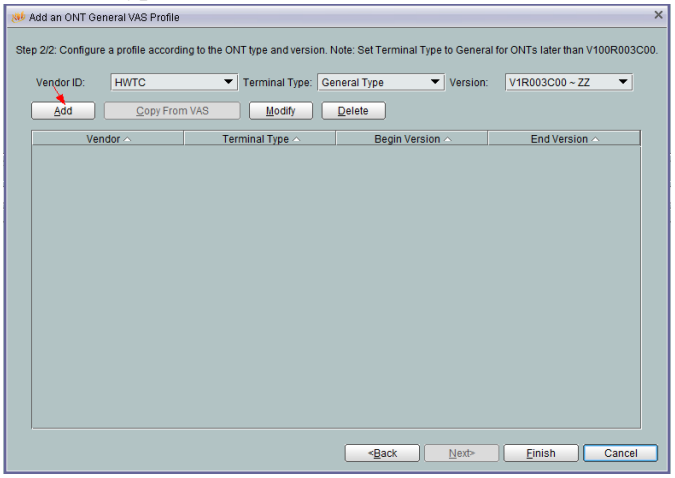
If **Interface ID** is **1**, port TEL1 on the ONT is bound. If **Interface ID** is **2**, port TEL2 on the ONT is bound.

Copyright © Huawei Technologies Co., Ltd.



h. Click **Next**.

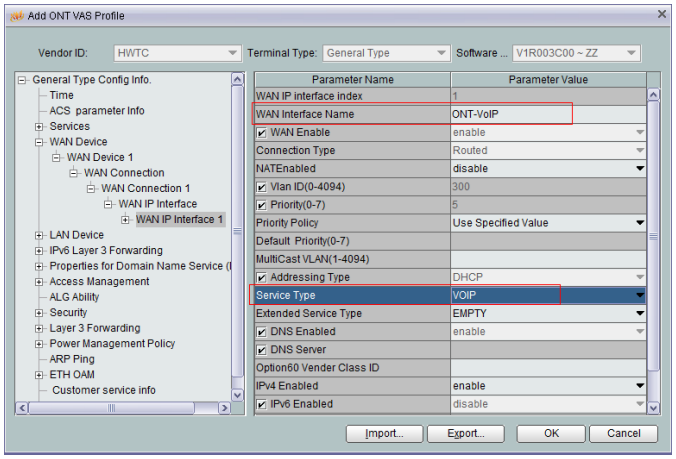
i. In the dialog box that is displayed, set **vendor ID** to **HWTC**, **Terminal Type** to **General Type**, and **Version** to **V1R003C00-ZZ**, click **Add**.



j. In the dialog box that is displayed, set the parameters.

- Choose **General Type Config Info** > **Services** > **Voice Service** > **Voice Service 1** > **Interface Configuration** > **Interface 1** from the navigation tree, and set **Region** to **China**.
- Choose **General Type Config Info** > **WAN Device** > **WAN Device 1** > **WAN Connection** > **WAN Connection 1** > **WAN IP Interface** > **WAN IP Interface 1** from the navigation tree, and set **WAN Interface Name** to **ONT-VoIP**, **Service Type** to **VOIP**.

Copyright © Huawei Technologies Co., Ltd.



k. Click **OK**.

2. **Bind a general VAS profile.**

   a. In the Main Topology, double-click the required OLT in the **Physical Root** navigation tree; or right-click the required OLT and choose **NE Explorer** from the shortcut menu.

   b. Choose **GPON** > **GPON Management** from the navigation tree.

   c. In the window on the right, choose **GPON ONU**.

   d. On the **GPON ONU** tab page, set the filter criteria or click to display the GPON ONUs.

   e. Select an ONT from the list, right-click, and choose **Bind General VAS Profile** from the shortcut menu. In the dialog box that is displayed, select the created profile, and click **OK** to complete profile binding.

3. **Configure the ONT VAS service.**

   a. On the **GPON ONU** tab page, select an ONT, right-click, and choose **Configure Value-Added Service** from the shortcut menu.

   b. Configure the domain name of the MG.

   Click the **Basic Parameters** tab in the dialog box that is displayed, select **Voice Service**, and set **MG Domain name** to **0100000001**.

   NOTE

   Domain Name is ONT's domain name registered with the MGC. It is globally unique. **MG Domain Name** in this example is ONT's password.

   c. Configure the terminal ID for the H.248 voice user.

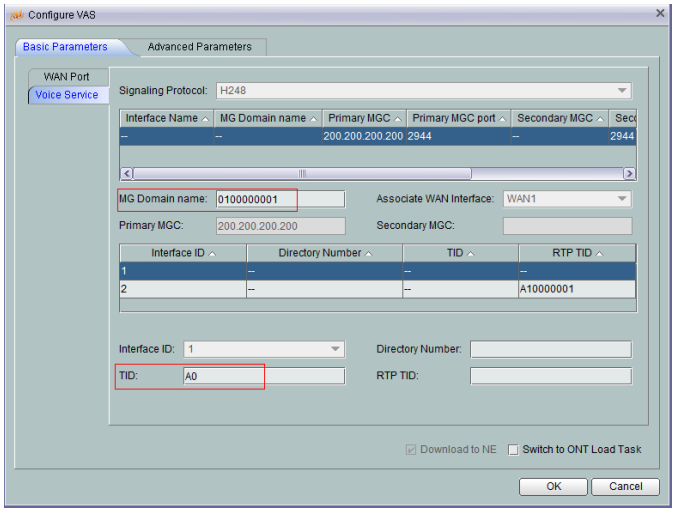
   Select the record where **Interface ID** is **1**, and set **TID** to **A0**. Select the record where **Interface ID** is **2**, and set **TID** to **A1**.

   NOTE

   Pay attention to the RTP TID configuration when the ONT is interconnected with a softswitch of other vendors. The terminal IDs **A0** and **A1** must be consistent with the corresponding configuration on the MGC.

   Do not configure **Directory Number**.

Copyright © Huawei Technologies Co., Ltd.



d. Click **OK**. The configurations take effect without the requirement of resetting the ONT.

----End

9.7.1.6 Configuring the H.248-based Voice Service (Through the CLI)

The OLT manages ONTs and applies VoIP configurations to the ONT using the OMCI protocol. This topic describes how to configure the H.248-based voice service.

Prerequisites

- The interface data and POTS user configuration data corresponding to the MG interface have been configured on the MGC.
- The OLT has been connected to the MGC. The OLT can ping the IP address of the MGC server successfully.
- The ONT has been added to the OLT. For details, see **9.7.1.3 Adding an ONT to an OLT**.
- Different voice services require different ONT software versions. Before the configuration, ensure that the current ONT software version supports H.248. For details, see relevant ONT manuals.
- The ONT software version of the H.248 voice service can be configured as V100R002C04 or later through the CLI.

Data Plan

Item	Data
ONT line profile	Profile name: ftth T-CONT ID: 4 GEM port ID: 12

Copyright © Huawei Technologies Co., Ltd.

Item	Data
VLAN plan	Single VLAN tag: ● VLAN ID: 300 ● VLAN type: smart ● VLAN attribute: common ● CVLAN=SVLAN VLAN translation policy: ● ONT: VLANs are configured for the ONTs on the same network in a unified manner, and the ONTs have the same C-VLAN. The ONT adds a C-VLAN tag to packets. ● OLT: transparently transmits the VLAN.
Voice parameter	IP address of the MGC server: 200.200.200.200/24 Port ID of the MGC server: 2944 MG Domain: 0100000001 or 0100000002

Procedure

Step 1 Configure a traffic profile.

Run the **display traffic table ip** command to query the existing traffic profiles in the system. If the existing traffic profiles in the system do not meet the requirements, run the **traffic table ip** command to add a traffic profile.

Step 2 Configure the mapping relationship between a GEM port and a VLAN.

The service flow of user VLAN 300 is mapped to GEM port 12 in the ONT line profile.

```
huawei(config)#ont-lineprofile gpon profile-name ftth
huawei(config-gpon-lineprofile-1)#gem mapping 12 2 vlan 300
huawei(config-gpon-lineprofile-1)#commit
huawei(config-gpon-lineprofile-1)#quit
```

Step 3 Create a service VLAN and add an upstream port to it.

Add upstream port 0/19/0 to VLAN 300.

```
huawei(config)#vlan 300 smart
huawei(config)#port vlan 300 0/19 0
```

Step 4 Create service flows.

Set the service VLAN to 300, GEM port ID to 12, and user VLAN to 300, and use traffic profile **ftth_voip**.

```
huawei(config)#service-port vlan 300 gpon 0/1/0 ont 1 gemport 12 multi-service
 user-vlan 300 inbound traffic-table name ftth_voip outbound traffic-table name
ftth_voip
huawei(config)#service-port vlan 300 gpon 0/1/0 ont 2 gemport 12 multi-service
 user-vlan 300 inbound traffic-table name ftth_voip outbound traffic-table name
ftth_voip
```


Copyright © Huawei Technologies Co., Ltd.

Step 5 Configure the mode of issuing VoIP services.

Run the **ont voip config-method** command to configure the mode of issuing VoIP services. If the mode of issuing VoIP services is not **default** or **omci**, run this command to set the mode to **default** or **omci**. You can run the **display ont info** command to query the mode of issuing VoIP services.

In this example, the mode is **default**.

Step 6 Configure ONT voice service profiles.

ONT voice service profiles include the interface common profile, MGC interface profile, and POTS port profile.

- Interface common profile: saves common attributes of an ONT voice interface, including the fax mode, fax/modem negotiation mode, and priority of the coding and decoding mode.
- MGC interface profile: saves the IP address or domain name of the MGC, protocol port ID of the MGC transport layer to which the MG interface belongs, and DSCP priority of media packets.
- POTS port profile: saves physical attributes of a POTS port on an ONT, including the impedance, transmitting gain, receiving gain, and signaling type of the POTS port.

1. Configure an interface common profile.

   Run the **display ont-mg-attribute-profile** command to query the existing interface common profile in the system. If the existing interface common profile in the system does not meet the requirements, run the **ont-mg-attribute-profile add** command to add an interface common profile.

   In this example, the default interface common profile, namely interface common profile 1 is used.

2. Configure an MGC interface profile.

   Run the **display ont-mgc-profile** command to query the existing MGC interface profile in the system. If the existing MGC interface profile in the system does not meet the requirements, run the **ont-mgc-profile add** command to add an MGC interface profile.

   Create MGC interface profile 2, set the IP address of the MGC to 200.200.200.200, and use default values for other parameters.

   ```
   huawei(config)#ont-mgc-profile add profile-id 2 primary-mgc 200.200.200.200
   ```

3. Configure a POTS port profile.

   Run the **display ont-pots-profile** command to query the existing POTS port profile in the system. If the existing POTS port profile in the system does not meet the requirements, run the **ont-pots-profile add** command to add a POTS port profile.

   In this example, the default POTS port profile, namely POTS port profile 1 is used.

Step 7 Configure the IP addresses of ONT SIP users.

For ONT 1 and ONT 2, configure the IP address obtaining mode to DHCP mode, set the management VLAN to VLAN 20, and use default values for other parameters.

```
huawei(config)#interface gpon 0/1
huawei(config-if-gpon-0/1)#ont ipconfig 0 1 dhcp vlan 20
huawei(config-if-gpon-0/1)#ont ipconfig 0 2 dhcp vlan 20
```

Step 8 Configure H.248 POTS users.

1. Add an H.248 interface and apply an MGC interface profile to the interface.

   For ONT 1 and ONT 2, set the MG ID to 1, apply MGC interface profile 2 to ONT 1 and ONT 2, and use default values for other parameters.

Copyright © Huawei Technologies Co., Ltd.

If parameters of an MGC interface profile are changed, the MGC interface profile must be reapplied to the ONT so that the changed parameters can take effect.

```
huawei(config-if-gpon-0/1)#if-h248 add 0 1 1 mgc-profile profile-id 2
huawei(config-if-gpon-0/1)#if-h248 add 0 2 1 mgc-profile profile-id 2
```

2. Add POTS users.

   For ONT 1 and ONT 2, create a POTS user, set the MG ID to 1 (identical to the MG ID of the H.248 interface), and set the physical terminal port ID to A0 and A1.

```
huawei(config-if-gpon-0/1)#mgpstnuser add 0 1 1 mgid 1 terminalid A0
huawei(config-if-gpon-0/1)#mgpstnuser add 0 2 1 mgid 1 terminalid A1
```

   Run the **display mgpstnuser attribute** command to check whether the configuration of the POTS user is properly set.

```
huawei(config-if-gpon-0/1)#display mgpstnuser attribute 0 1 1

---------------------------------------------------------------------------
  F/S/P                     : 0/1/0
  ONT ID                    : 1
  Port ID                   : 1

  MG ID                     : 1
  Terminal ID               : A0
...//The rest of the response information is omitted.

huawei(config-if-gpon-0/1)#display mgpstnuser attribute 0 2 1

---------------------------------------------------------------------------
  F/S/P                     : 0/1/0
  ONT ID                    : 2
  Port ID                   : 1

  MG ID                     : 1
  Terminal ID               : A1
...//The rest of the response information is omitted.
```

Step 9 Apply ONT voice service profiles

After ONT voice service profiles are applied, if parameters in those profiles are changed, those profiles must be reapplied so that the changed parameters can take effect.

1. Apply an interface common profile.

   Run the **if-h248 attribute** command to apply an interface common profile to an H.248 interface or configure the interface customized parameters, or run the **ont-if-h248 bat-apply** command to bulk apply the interface common profiles to H.248 interfaces. If you use these two commands to apply the interface common profiles or configure the interface customized parameters repeatedly, the last configurations take effect.

   In this example, the default interface common profile, namely interface common profile 1 is used.

2. Apply a POTS port profile.

   Run the **pstnport electric** command to apply a POTS port profile to an H.248 interface or configure the interface customized parameters, or run the **ont-pstnport electric bat-apply** command to bulk apply the POTS port profiles to H.248 interfaces. If you use these two commands to apply the POTS port profiles or configure the interface customized parameters repeatedly, the last configurations take effect.

   In this example, the default POTS port profile, namely POTS port profile 1 is used.

Step 10 (Optional) Configure the H.248 user codec.

Copyright © Huawei Technologies Co., Ltd.

Run the **mgpstnuser codec** command to configure the H.248 user codec. The H.248 user codec will not be configured independently in this example.

Step 11 Save the data.

```
huawei(config)#save
```

----End

9.7.1.7 Configuring the SIP-based Voice Service (on a Web Page or the U2000)

The OLT is connected to the remote ONT through a GPON port to provide users with the SIP-based high-quality and low-cost VoIP service.

Prerequisites

- The SIP interface data and POTS user configuration data corresponding to the MG interface have been configured on the SIP server.
- The connection between the OLT and the SIP server is set up. The OLT can ping the IP address of the SIP server successfully.
- The ONT has been added to the OLT. For details, see **9.7.1.3 Adding an ONT to an OLT**.
- Different voice services require different ONT software versions. Before the configuration, ensure that the current ONT software version supports SIP. For details, see relevant ONT manuals.

Data Plan

Item	Data
ONT line profile	Profile name: ftth T-CONT ID: 4 GEM port ID: 12
VLAN plan	Single VLAN tag: ● VLAN ID: 300 ● VLAN type: smart ● VLAN attribute: common ● CVLAN=SVLAN VLAN translation policy: ● ONT: VLANs are configured for the ONTs on the same network in a unified manner, and the ONTs have the same C-VLAN. The ONT adds a C-VLAN tag to packets. ● OLT: transparently transmits the VLAN.

Copyright © Huawei Technologies Co., Ltd.

Item	Data
Voice parameter	IP address of the SIP server: 200.200.200.200/24 Port ID of the SIP server: 5060 Home domain name: huawei.com User phone number 1: 77730010 User phone number 2: 77730020

Procedure

- Configure the OLT.
  1. Configure a traffic profile.

     Run the **display traffic table ip** command to query the existing traffic profiles in the system. If the existing traffic profiles in the system do not meet the requirements, run the **traffic table ip** command to add a traffic profile.

     Set the profile name to **ftth_voip** and do not limit the upstream and downstream rates. Set the priority to **5** and packets are scheduled according to the priority carried.

     ```
     huawei(config)#traffic table ip name ftth_voip cir off priority 5 priority-policy
      local-setting
     ```

  2. Configure the mapping relationship between a GEM port and a VLAN.

     The service flow of user VLAN 300 is mapped to GEM port 12 in the ONT line profile.

     ```
     huawei(config)#ont-lineprofile gpon profile-name ftth
     huawei(config-gpon-lineprofile-1)#gem mapping 12 2 vlan 300
     huawei(config-gpon-lineprofile-1)#commit
     huawei(config-gpon-lineprofile-1)#quit
     ```

  3. Create a service VLAN and add an upstream port to it.

     Add upstream port 0/19/0 to VLAN 300.

     ```
     huawei(config)#vlan 300 smart
     huawei(config)#port vlan 300 0/19 0
     ```

  4. Create service flows.

     Set the service VLAN to 300, GEM port ID to 12, and user VLAN to 300, and use traffic profile **ftth_voip**.

     ```
     huawei(config)#service-port vlan 300 gpon 0/1/0 ont 1 gemport 12 multi-service
      user-vlan 300 inbound traffic-table name ftth_voip outbound traffic-table name
     ftth_voip
     huawei(config)#service-port vlan 300 gpon 0/1/0 ont 2 gemport 12 multi-service
      user-vlan 300 inbound traffic-table name ftth_voip outbound traffic-table name
     ftth_voip
     ```

  5. Enable the ARP proxy function.

     Voice media streams for different users of the same SVLAN fail to interchange because the service ports of the smart VLAN are isolated from each other. Therefore, the ARP proxy function needs to be enabled on the OLT.

Copyright © Huawei Technologies Co., Ltd.

```
huawei(config)#arp proxy enable
huawei(config)#interface vlanif 300
huawei(config-if-vlanif300)#arp proxy enable
huawei(config-if-vlanif300)#quit
```

6. Save the data.

```
huawei(config)#save
```

- Configure the ONT on the Web page.

  Log in to the Web page and then configure the ONT on the Web page.

  1. Configure the IP address of the PC network adapter to be in the same network segment with the IP address of the local maintenance Ethernet port on the ONT (default: 192.168.100.1).
  2. Open the Web browser, and enter the IP address (https://192.168.100.1:80 or http://192.168.100.1) (https with high priority is recommended) of the local maintenance Ethernet port on the ONT. In the login window that is displayed, enter the user name (default telecomadmin) and password (default admintelecom) of the administrator. After the password is authenticated, the web configuration window is displayed.

  NOTE

  - The following configuration procedure is for scenarios with the bridging ONT. For scenarios with the bridging ONT+HGW, configure the voice service on the HGW but not on the ONT. For detailed configurations, see the HGW Configuration Guide.
  - The Web page for configuring ONT varies with ONT versions, but the parameter configuration is the same. For details, see relevant ONT manuals.

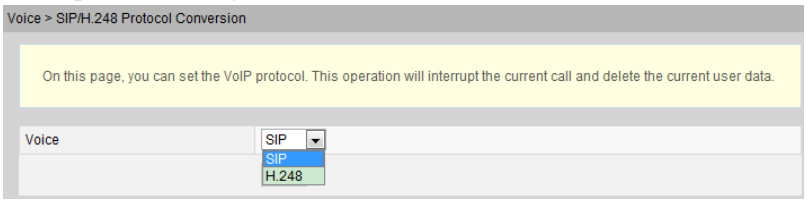
  1. **Optional:** Configure the voice protocol.

     NOTE

     The default voice protocol is SIP. If the protocol is not changed, skip this step.

     a. Choose **Voice** > **SIP/H.248 Protocol Conversion**.

     b. In the pane on the right, set **Voice** to **SIP**.

     c. Click **Apply**.

  2. Configure parameters for the voice WAN interface.

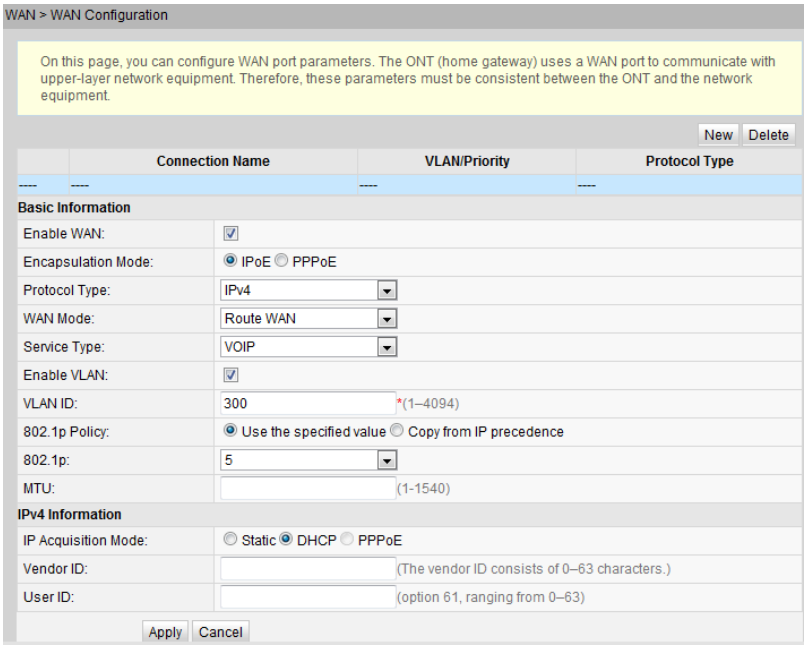
     a. Choose **WAN** > **WAN Configuration**.

     b. In the right pane, click **New**. In the dialog box that is displayed, set the parameters as follows:

        - Select **Enable WAN Connection** to enable the new WAN connection.
        - Set **Encapsulation mode** to **IPoE**.
        - Set **Service Type** to **VOIP**. (For configuring the VoIP service, VoIP or a combination containing VoIP needs to be selected.)
        - Set **WAN mode** to **Route WAN**.
        - Select **Enable VLAN**.

Copyright © Huawei Technologies Co., Ltd.

- Set **VLAN ID** to **300**. (The VLAN ID of the ONT must be the same as the user-side VLAN ID configured on the OLT.)
- Set **802.1p** to **5**.
- Set **IP Acquisition Mode** to **DHCP**.



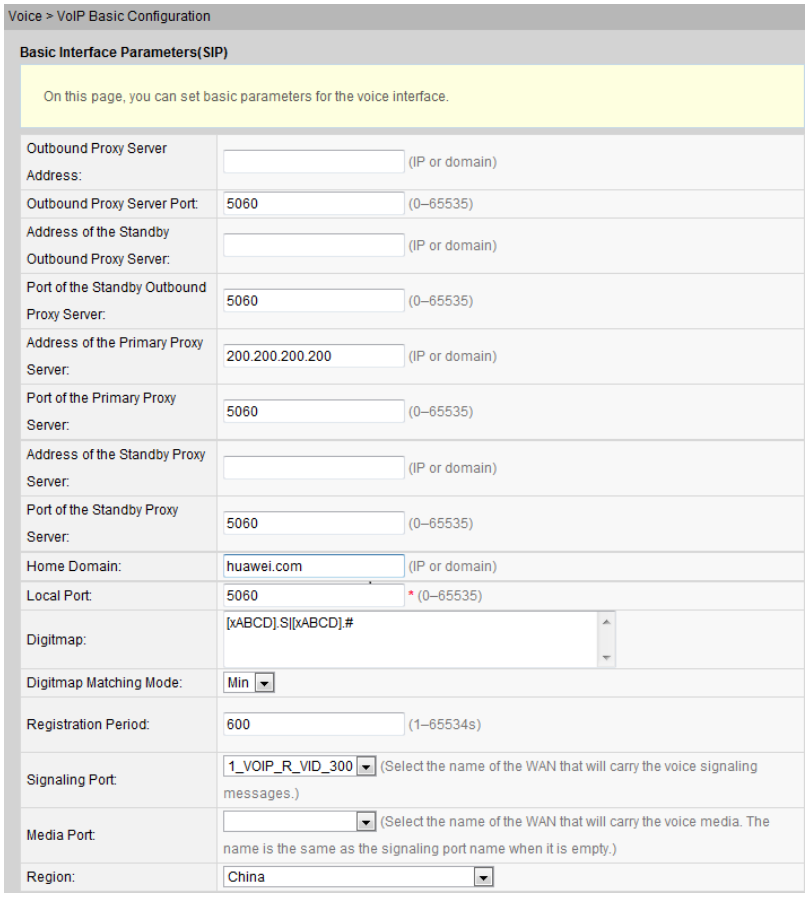
c. Click **Apply**.

3. Configure parameters for the SIP-based voice interface.
   a. Choose **Voice** > **VoIP Basic Configuration**.
   b. In the **Basic Interface Parameters(SIP)** window, configure the parameters as follows:
      - Set **Address of the Primary Proxy Server** to **200.200.200.200**.
      - Set **Home Domain** to **huawei.com**.
      - Set **Region** to **China**.
      - Set **Signaling Port** to **1_VOIP_R_VID_300**.

      NOTE

      - The parameters of the SIP-based voice interface must be consistent with the corresponding configuration on the softswitch.
      - If dual-homing is configured, **Address of the Standby Proxy Server** must be configured.
      - If **Signaling Port** is empty, the parameter value is the same as **Media Port**. If the upper-layer network requires isolation of media streams from signaling streams, create different traffic streams for the media streams and signaling streams on the OLT, create different WAN ports on the ONT, and bind the created WAN ports to **Media Port** and **Signaling Port**. When the packet is forwarded from two WAN ports, the configured VLAN is carried by default.

Copyright © Huawei Technologies Co., Ltd.



c. Configure parameters for the SIP-based voice users.

a. Choose **Voice** > **VoIP Basic Configuration**.

b. In the **Basic User Parameters(SIP)** window, set parameters for voice user 1 as follows:

- Select **Enable User** to enable the voice user configuration.
- Set **Registration User Name** to **77730010**.
- Set **Associated POTS Port** to **1**.
- Set **Authentication User Name** to **+8675577730010@huawei.com**.
- Set **Password** to **iadtest1**.

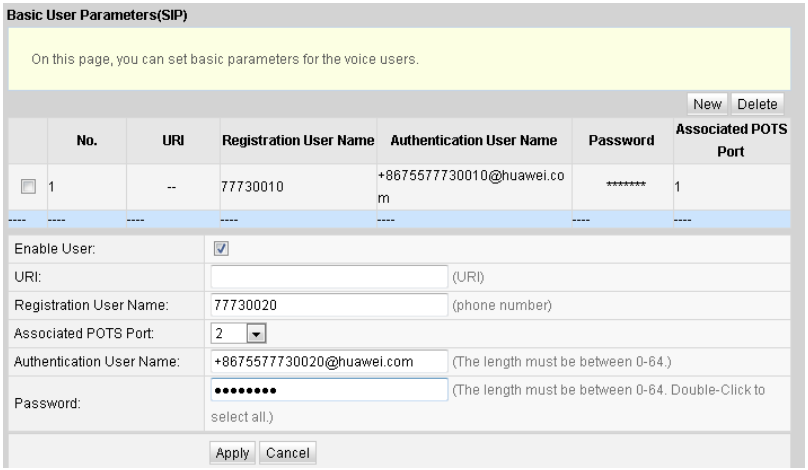
Click **New** to add voice user 2, and set the parameters for voice user 2 as follows:

- Select **Enable User** to enable the voice user configuration.
- Set **Registration User Name** to **77730020**.
- Set **Associated POTS Port** to **2**.
- Set **Authentication User Name** to **+8675577730020@huawei.com**.
- Set **Password** to **iadtest2**.

Copyright © Huawei Technologies Co., Ltd.

NOTE

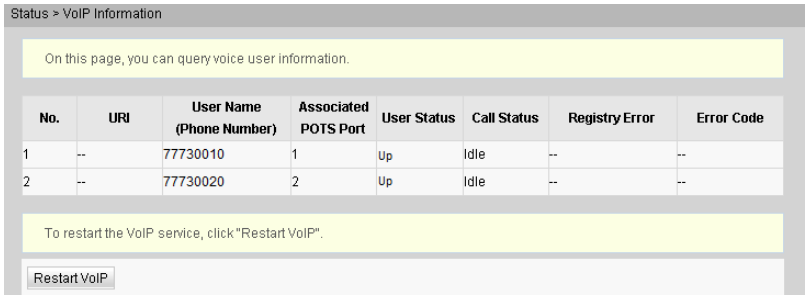
- The parameters of the SIP-based voice user must be consistent with the corresponding configuration on the softswitch.
- If **Associated POTS Port** is **1**, port TEL1 on the ONT is bound. If **Associated POTS Port** is **2**, port TEL2 on the ONT is bound.



d. Click **Apply**.

4. Check the registration status of the voice user.

   Choose **Status** > **VoIP Information**. In the right pane, **User Status** is **Up**.



- Configure the ONT on the U2000.

  NOTE

  - The following configuration procedure is for scenarios with the bridging ONT. For scenarios with the bridging ONT+HGW, configure the voice service on the HGW but not on the ONT. For detailed configurations, see the HGW Configuration Guide.
  - The window for configuring ONT value-added service (VAS) profiles varies with ONT versions, but the parameter configuration is the same. For details, see relevant ONT manuals.

  1. Configure a general VAS profile for the ONT.

     a. From the main menu, choose **Configuration** > **Access Profile Management**. In the navigation tree of the tab page that is displayed, choose **PON Profile** > **ONT VAS Profile**.

     b. On the **General ONT VAS Profile** tab page, right-click, and choose **Add** from the shortcut menu.

     c. In the dialog box that is displayed, set **Name** to **ONT-VoIP**.

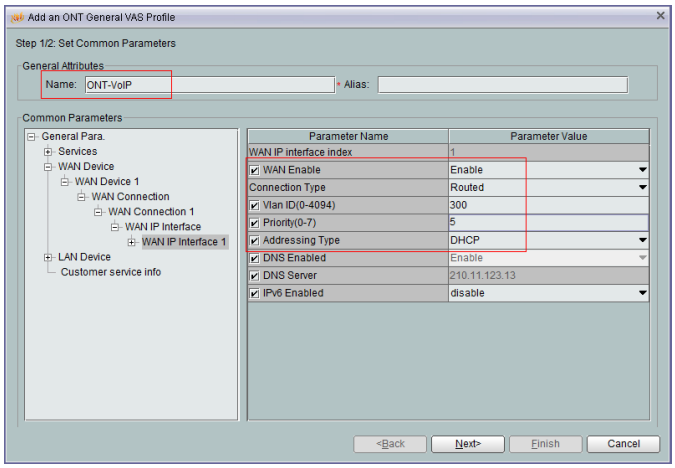
     d. Configure the parameters of a voice WAN port.

Copyright © Huawei Technologies Co., Ltd.

a. In the navigation tree, choose **General Para** > **WAN Device** > **WAN Device 1** > **WAN Connection**. Select **WAN Connection**, right-click, and choose **Add IP Connection** from the shortcut menu.

b. Select **WAN IP Interface 1** and enter (or select) a proper value.

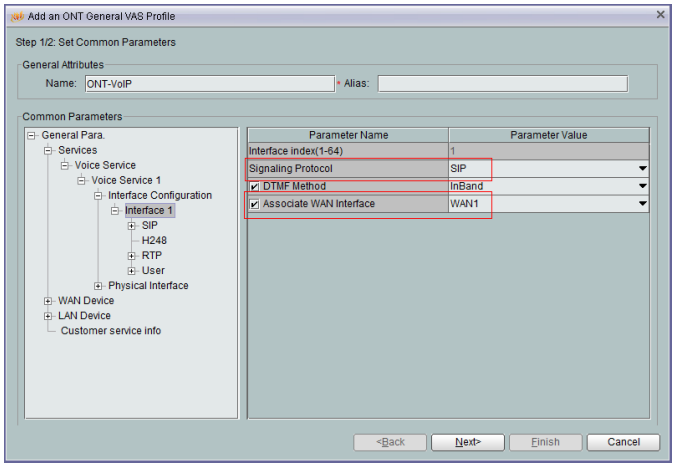
- WAN Enable: enable
- Connection Type: Routed
- VLAN ID: 300 (The VLAN ID of the ONT must be the same as the user-side VLAN ID configured on the OLT.)
- Priority: 5
- Addressing Type: DHCP



e. Configure parameters of the voice protocol.

In the navigation tree, choose **General Para** > **Services** > **Voice Service** > **Voice Service 1** > **Interface configuration** > **Interface 1**. Select **Interface 1** and select a proper value.

- Signaling Protocol: SIP
- Associate WAN Interface: WAN1 (binding the created voice WAN port)



f. Configure SIP protocol parameters.

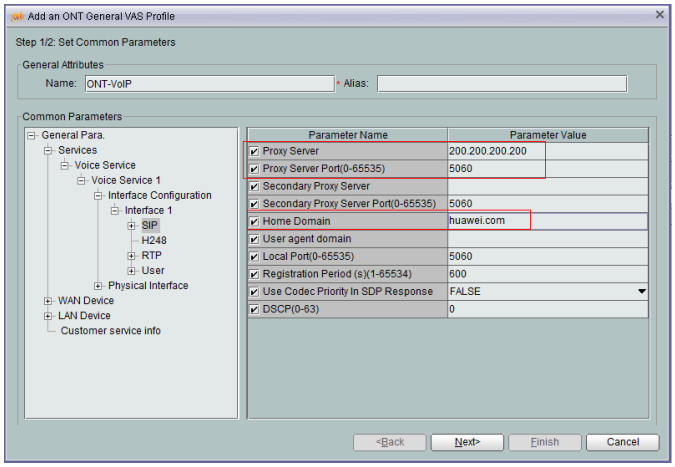
In the navigation tree, choose **General Para** > **Services** > **Voice Service** > **Voice Service 1** > **Interface configuration** > **Interface 1** > **SIP**. Select **SIP** and enter (or select) a proper value.

Copyright © Huawei Technologies Co., Ltd.

- Proxy Server: 200.200.200.200
- Server Port: 5060
- Home Domain: huawei.com

NOTE

If dual-homing is configured, **Secondary Proxy Server** must be set.



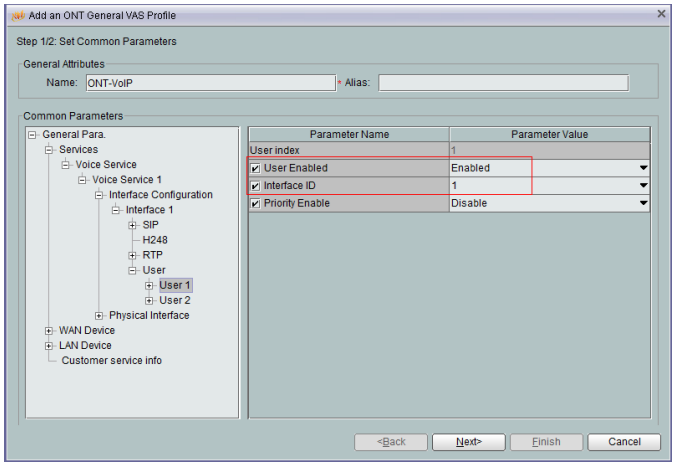
g. Configure the voice users.

a. In the navigation tree, choose **General Para** > **Services** > **Voice Service** > **Voice Service 1** > **Interface configuration** > **Interface 1** > **User**. Right-click **User** and choose **Add** from the shortcut menu.

b. Select **User 1** under the **User** node. In the right pane, set **User Enabled** to **Enable**, and **Interface ID** to **1**. Then, select **User 2** under the **User** node. In the right pane, set **User Enabled** to **Enable**, and **Interface ID** to **2**.

NOTE

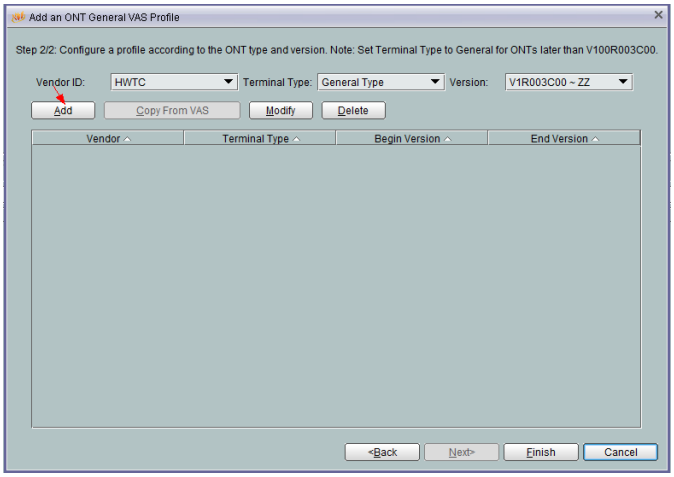
If **Interface ID** is **1**, port TEL1 on the ONT is bound. If **Interface ID** is **2**, port TEL2 on the ONT is bound.



h. Click **Next**.

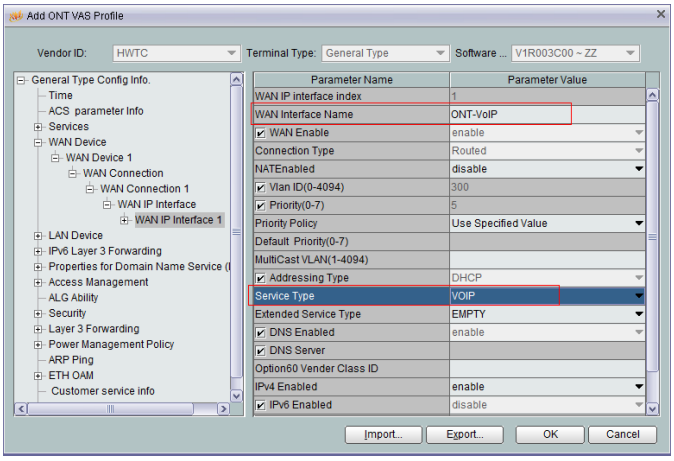
i. In the dialog box that is displayed, set **vendor ID** to **HWTC**, **Terminal Type** to **General Type**, and **Version** to **V1R003C00-ZZ**, click **Add**.

Copyright © Huawei Technologies Co., Ltd.



j. In the dialog box that is displayed, set the parameters.

- Choose **General Type Config Info** > **Services** > **Voice Service** > **Voice Service 1** > **Interface Configuration** > **Interface 1** from the navigation tree, and set **Region** to **China**.
- Choose **General Type Config Info** > **WAN Device** > **WAN Device 1** > **WAN Connection** > **WAN Connection 1** > **WAN IP Interface** > **WAN IP Interface 1** from the navigation tree, and set **WAN Interface Name** to **ONT-VoIP**, **Service Type** to **VOIP**.



k. Click **OK**.

2. **Bind a general VAS profile.**

a. In the Main Topology, double-click the required OLT in the **Physical Root** navigation tree; or right-click the required OLT and choose **NE Explorer** from the shortcut menu.

b. Choose **GPON** > **GPON Management** from the navigation tree.

c. In the window on the right, choose **GPON ONU**.

d. On the **GPON ONU** tab page, set the filter criteria or click to display the GPON ONUs.

e. Select an ONT from the list, right-click, and choose **Bind General VAS Profile** from the shortcut menu. In the dialog box that is displayed, select the created profile, and click **OK** to complete profile binding.

Copyright © Huawei Technologies Co., Ltd.

3. **Configure the ONT VAS service.**

   a. On the **GPON ONU** tab page, select an ONT, right-click, and choose **Configure Value-Added Service** from the shortcut menu.

   b. Configure parameters for the SIP-based voice users.

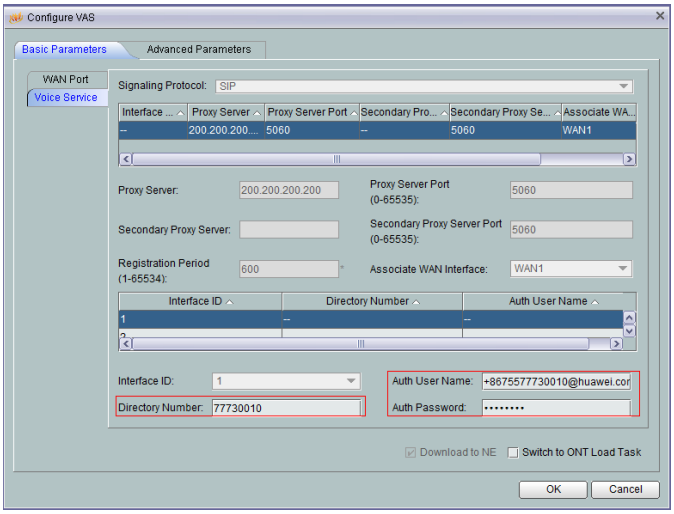
   NOTE

   The parameters of the SIP-based voice user must be consistent with the corresponding configuration on the softswitch.

      a. Click the **Basic Parameters** tab in the dialog box that is displayed, select **Voice Service**. Select **User 1** and set **Directory Number** to **77730010**.

      b. Select **SIP** below **User 1** and enter a proper value.

         - Auth User Name: +8675577730010@huawei.com
         - Auth Password: iadtest1



      c. Set parameters of **User 2** using the same method.

         - Directory Number: 77730020
         - Auth User Name: +8675577730020@huawei.com
         - Auth Password: iadtest2

   c. Click **OK**. The configurations take effect without the requirement of resetting the ONT.

----End

9.7.1.8 Configuring the SIP-based Voice Service (Through the CLI)

The OLT manages ONTs and applies VoIP configurations to the ONT using the OMCI protocol. This topic describes how to configure the SIP-based voice service.

Prerequisites

- The SIP interface data and POTS user configuration data corresponding to the MG interface have been configured on the SIP server.
- The connection between the OLT and the SIP server is set up. The OLT can ping the IP address of the SIP server successfully.

Copyright © Huawei Technologies Co., Ltd.

- The ONT has been added to the OLT. For details, see **9.7.1.3 Adding an ONT to an OLT**.
- Different voice services require different ONT software versions. Before the configuration, ensure that the current ONT software version supports SIP. For details, see relevant ONT manuals.
- The ONT software version of the SIP voice service can be configured as V100R002C04 or later through the CLI.

Data Plan

Item	Data
ONT line profile	Profile name: ftth T-CONT ID: 4 GEM port ID: 12
VLAN plan	Single VLAN tag: ● VLAN ID: 300 ● VLAN type: smart ● VLAN attribute: common ● CVLAN=SVLAN VLAN translation policy: ● ONT: VLANs are configured for the ONTs on the same network in a unified manner, and the ONTs have the same C-VLAN. The ONT adds a C-VLAN tag to packets. ● OLT: transparently transmits the VLAN.
Voice parameter	IP address of the SIP server: 200.200.200.200/24 Port ID of the SIP server: 5060 Home domain name: huawei.com User phone number 1: 77730010 User phone number 2: 77730020

Procedure

Step 1 Configure a traffic profile.

Run the **display traffic table ip** command to query the existing traffic profiles in the system. If the existing traffic profiles in the system do not meet the requirements, run the **traffic table ip** command to add a traffic profile.

Step 2 Configure the mapping relationship between a GEM port and a VLAN.

The service flow of user VLAN 300 is mapped to GEM port 12 in the ONT line profile.

```
huawei(config)#ont-lineprofile gpon profile-name ftth
huawei(config-gpon-lineprofile-1)#gem mapping 12 2 vlan 300
```


Copyright © Huawei Technologies Co., Ltd.

```
huawei(config-gpon-lineprofile-1)#commit
huawei(config-gpon-lineprofile-1)#quit
```

Step 3 Create a service VLAN and add an upstream port to it.

Add upstream port 0/19/0 to VLAN 300.

```
huawei(config)#vlan 300 smart
huawei(config)#port vlan 300 0/19 0
```

Step 4 Create service flows.

Set the service VLAN to 300, GEM port ID to 12, and user VLAN to 300, and use traffic profile **ftth_voip**.

```
huawei(config)#service-port vlan 300 gpon 0/1/0 ont 1 gemport 12 multi-service
 user-vlan 300 inbound traffic-table name ftth_voip outbound traffic-table name
ftth_voip
huawei(config)#service-port vlan 300 gpon 0/1/0 ont 2 gemport 12 multi-service
 user-vlan 300 inbound traffic-table name ftth_voip outbound traffic-table name
ftth_voip
```

Step 5 Configure the mode of issuing VoIP services.

Run the **ont voip config-method** command to configure the mode of issuing VoIP services. If the mode of issuing VoIP services is not **default** or **omci**, run this command to set the mode to **default** or **omci**. You can run the **display ont info** command to query the mode of issuing VoIP services.

In this example, the mode is **default**.

Step 6 Configure ONT voice service profiles.

ONT voice service profiles include the interface common profile, SIP agent profile, SIP service data profile, POTS port profile, and digitmap profile.

- Interface common profile: saves common attributes of an ONT voice interface, including the fax mode, fax/modem negotiation mode, and priority of the coding and decoding mode.
- SIP agent profile: saves the SIP agent information about an ONT, including the IP address and domain name of the SIP agent server and attributes of media packets and signaling packets.
- SIP service data profile: saves the data information about ONT voice services, including the rights of the call waiting service, three-party service, call forwarding service, and call holding service.
- POTS port profile: saves physical attributes of a POTS port on an ONT, including the impedance, transmitting gain, receiving gain, and signaling type of the POTS port.
- Digitmap profile: saves the digitmap information about an ONT, including the timeout time of the digitmap timer and the digitmap format.

1. Configure an interface common profile.

   Run the **display ont-mg-attribute-profile** command to query the existing interface common profile in the system. If the existing interface common profile in the system does not meet the requirements, run the **ont-mg-attribute-profile add** command to add an interface common profile.

   In this example, the default interface common profile, namely interface common profile 1 is used.

2. Configure an SIP agent profile.

Copyright © Huawei Technologies Co., Ltd.

Run the **display ont-sipagent-profile** command to query the existing SIP agent profile in the system. If the existing SIP agent profile in the system does not meet the requirements, run the **ont-sipagent-profile add** command to add an SIP agent profile.

Create SIP agent profile 2, set the IP address of the SIP server to 200.200.200.200, and use default values for other parameters.

```
huawei(config)#ont-sipagent-profile add profile-id 2 proxy-server
200.200.200.200
```

3. Configure an SIP service data profile.

   Run the **display ont-siprightflag-profile** command to query the existing SIP agent profile in the system. If the existing SIP service data profile in the system does not meet the requirements, run the **ont-siprightflag-profile add** command to add an SIP service data profile.

   In this example, the default SIP service data profile, namely SIP service data profile 1 is used.

4. Configure a POTS port profile.

   Run the **display ont-pots-profile** command to query the existing POTS port profile in the system. If the existing POTS port profile in the system does not meet the requirements, run the **ont-pots-profile add** command to add a POTS port profile.

   In this example, the default POTS port profile, namely POTS port profile 1 is used.

5. Configure a digitmap profile.

   Run the **display ont-digitmap-profile** command to query the existing digitmap profile in the system. If the existing digitmap profile in the system does not meet the requirements, run the **ont-digitmap-profile add** command to add a digitmap profile.

   In this example, the default digitmap profile, namely digitmap profile 1 is used.

Step 7 Configure an IP address for an ONT SIP user.

For ONT 1 and ONT 2, configure the IP address obtaining mode to the DHCP mode, set the management VLAN to VLAN 20, and use default values for other parameters.

```
huawei(config)#interface gpon 0/1
huawei(config-if-gpon-0/1)#ont ipconfig 0 1 dhcp vlan 20
huawei(config-if-gpon-0/1)#ont ipconfig 0 2 dhcp vlan 20
```

Step 8 Configure SIP POTS users.

1. Add an SIP interface and apply an SIP agent profile to the interface.

   For ONT 1 and ONT 2, set the MG ID to 1, apply SIP agent profile 2 to ONT 1 and ONT 2, and use default values for other parameters.

   If parameters in an SIP agent profile are changed, the SIP agent profile must be reapplied to the ONT so that the changed parameters can take effect.

   ```
   huawei(config-if-gpon-0/1)#if-sip add 0 1 1 sipagent-profile profile-id 2
   huawei(config-if-gpon-0/1)#if-sip add 0 2 1 sipagent-profile profile-id 2
   ```

2. Add POTS users.

   For ONT 1 and ONT 2, set the MG ID to 1 (identical to the MG ID of the added SIP interface), create two POTS users named huawei1 and huawei2, set passwords to user1 and user2, set their phone numbers to 77730010 and 77730020 and use default values for other parameters.

   ```
   huawei(config-if-gpon-0/1)#sippstnuser add 0 1 1 mgid 1 username huawei1 telno
   77730010
   huawei(config-if-gpon-0/1)#sippstnuser add 0 2 1 mgid 1 username huawei2 telno
   77730020
   ```


Copyright © Huawei Technologies Co., Ltd.

Run the **display sippstnuser attribute** command to check whether the configuration of the POTS user is properly set.

```
huawei(config-if-gpon-0/1)#display sippstnuser attribute 0 1 1

--------------------------------------------------------------------------------
  F/S/P                       : 0/1/0
  ONT ID                      : 1
  Port ID                     : 1

  MG ID                       : 1
  Telephone NO.               : 77730010
  User name                   : huawei1
  Password                    : user1
...//The rest of the response information is omitted.

huawei(config-if-gpon-0/1)#display sippstnuser attribute 0 2 1

--------------------------------------------------------------------------------
  F/S/P                       : 0/1/0
  ONT ID                      : 2
  Port ID                     : 1

  MG ID                       : 1
  Telephone NO.               : 77730020
  User name                   : huawei2
  Password                    : user2
...//The rest of the response information is omitted.
```

Step 9 Apply and bind an ONT voice service profile to an SIP interface

Currently, the interface common profile, SIP agent profile, SIP service data profile, and POTS port profile can be applied to an SIP interface, and the digitmap profile can be bound to an SIP interface.

For profiles that can be applied to an SIP interface, if parameters in those profiles are changed, those profiles must be reapplied to the SIP interface so that the changed parameters can take effect. For profiles that can be bound to an SIP interface, if parameters in those profiles are changed, those profiles do not need to be rebound to the SIP interface and the changed parameters can take effect.

The method for applying an SIP agent profile is introduced in **Step 8.1**. The following will introduce the methods for applying an interface common profile, an SIP service data profile, and a POTS port profile, and the method for binding a digitmap to an SIP interface.

1. Apply an interface common profile.

   Run the **if-sip attribute** command to apply an interface common profile to an SIP interface or configure the interface customized parameters, or run the **ont-if-sip bat-apply from** command to bulk apply the interface common profiles to SIP interfaces. If you use these two commands to apply the interface common profiles or configure the interface customized parameters repeatedly, the last configurations take effect.

   In this example, the default interface common profile, namely interface common profile 1 is used.

2. Apply an SIP service data profile.

   Run the **sippstnuser rightflag** command to apply an SIP service data profile to an SIP interface or configure the interface customized parameters, or run the **ont-sippstnuser bat-apply from** command to bulk apply the SIP service data profiles to SIP interfaces. If you use these two commands to apply the SIP service data profiles or configure the interface customized parameters repeatedly, the last configurations take effect.

Copyright © Huawei Technologies Co., Ltd.

In this example, the default SIP service data profile, namely SIP service data profile 1 is used.

3. Apply a POTS port profile.

   Run the **pstnport electric** command to apply a POTS port profile to an SIP interface or configure the interface customized parameters, or run the **ont-pstnport electric bat-apply** command to bulk apply the POTS port profiles to SIP interfaces. If you use these two commands to apply the POTS port profiles or configure the interface customized parameters repeatedly, the last configurations take effect.

   In this example, the default POTS port profile, namely POTS port profile 1 is used.

4. Bind a digitmap profile.

   Run the **sippstnuser digitmap** command to bind a digitmap profile to an SIP interface, or run the **ont-sippstnuser bat-bind from** command to bulk apply the digitmap profiles to SIP interfaces. If you use these two commands to bind the SIP service data profiles to SIP ports repeatedly, the last configurations take effect.

   In this example, the default digitmap profile, namely digitmap profile 1 is used.

Step 10 (Optional) Configure the SIP user codec.

Run the **sippstnuser codec** command to configure the SIP user codec. The SIP user codec will not be configured independently in this example.

Step 11 Save the data.

```
huawei(config)#save
```

----End

9.7.1.9 Configuring the BTV Service

The OLT is connected to the remote bridging ONT through a GPON port to provide users with the multicast service.

Prerequisites

- The OLT is connected to the BRAS and the multicast source.
- The VLAN of the LAN switch port connected to the OLT is the same as the upstream VLAN of the OLT.
- The ONT has been added to the OLT. For details, see **9.7.1.3 Adding an ONT to an OLT**.

Data Plan

Table 9-3 Data plan

Item	Data
ONT line profile	Profile name: ftth T-CONT ID: 4 GEM port ID: 13

Copyright © Huawei Technologies Co., Ltd.

Item	Data
Traffic profile	ID: 8 802.1p priority: 4 CIR: off (unlimited) Priority-based scheduling policy: local-setting
VLAN Plan	Single VLAN tag: ● SVLAN ID: 1000 ● MVLAN ID: 1000 ● VLAN type: smart ● VLAN attribute: common VLAN translation policy: ● ONT: duplicates packets based on user ports and multicast VLANs (MVLANs) are stripped off downstream. ● OLT: duplicates multicast packets based on PON ports with MVLAN unchanged.
Multicast service data	Multicast protocol: IGMP proxy Multicast version: IGMPv2 Multicast program: dynamic obtaining mode

Procedure

- Configure the OLT.
  1. Configure a traffic profile.

     Configure traffic profile 8. Set the CIR to off (unlimited), priority to 4, and priority-based scheduling policy to local-setting (that is, queues are scheduled based on the priority specified in the profile).

     NOTE

     Run the **display traffic table ip** command to query the existing traffic profiles in the system. If the existing traffic profiles in the system do not meet the requirements, run the **traffic table ip** command to add a traffic profile.

     ```
     huawei(config)#traffic table ip index 8 cir off priority 4 priority-
     policy
     local-setting
     ```

  2. Configure the mapping relationship between a GEM port and an Ethernet port on the ONT.

     If the ONT is connected to the STB through Ethernet port 2, map the service flow of Ethernet port 2 to GEM port 13 in the ONT line profile.

     ```
     huawei(config)#ont-lineprofile gpon profile-name ftth
     huawei(config-gpon-lineprofile-1)#mapping mode port
     huawei(config-gpon-lineprofile-1)#gem mapping 13 1 eth 2
     ```


Copyright © Huawei Technologies Co., Ltd.

```
huawei(config-gpon-lineprofile-1)#commit
huawei(config-gpon-lineprofile-1)#quit
```

3. Configure the VLAN of the Ethernet port on the ONT.

   If the ONT is connected to the STB through Ethernet port 2, add Ethernet port 2 to VLAN 1000.

```
huawei(config)#ont-srvprofile gpon profile-name ftth
huawei(config-gpon-srvprofile-1)#port vlan eth 2 1000
huawei(config-gpon-srvprofile-1)#multicast-forward untag
huawei(config-gpon-srvprofile-1)#commit
huawei(config-gpon-srvprofile-1)#quit
```

4. Configure the native VLAN of the ONT port.

   If the ONT is connected to the STB through Ethernet port 2, the native VLAN ID is 1000.

```
huawei(config)#interface gpon 0/1
huawei(config-if-gpon-0/1)#ont port native-vlan 0 1 eth 2 vlan 1000
huawei(config-if-gpon-0/1)#ont port native-vlan 0 2 eth 2 vlan 1000
huawei(config-if-gpon-0/1)#quit
```

5. Create a service VLAN and add an upstream port to it.

   Add upstream port 0/19/0 to VLAN 1000.

```
huawei(config)#vlan 1000 smart
huawei(config)#port vlan 1000 0/19 0
```

6. Create service flows.

   Set the service VLAN to 1000, GEM port ID to 13, and user VLAN to 1000, and use traffic profile 8.

```
huawei(config)#service-port 1 vlan 1000 gpon 0/1/0 ont 1 gemport 13 multi-
service
 user-vlan 1000 rx-cttr 8 tx-cttr 8
huawei(config)#service-port 2 vlan 1000 gpon 0/1/0 ont 2 gemport 13 multi-
service
 user-vlan 1000 rx-cttr 8 tx-cttr 8
```

7. Create an MVLAN and configure the IGMP version.

   Set the IGMP version for the MVLAN to IGMPv2.

```
huawei(config)#multicast-vlan 1000
huawei(config-mvlan1000)#igmp version v2
  This operation will delete all IPv4 programs with source IP addresses in
the
current multicast VLAN
  Are you sure to change current IGMP version? (y/n)[n]:y
  Command is being executed. Please wait...
  Command has been executed successfully
```

8. Configure a program library.

   Set the mode for obtaining multicast programs to dynamic.

   NOTE

   You can set the mode for obtaining multicast programs to dynamic only when the IGMP mode is off.

```
huawei(config-mvlan1000)#igmp mode off
  Are you sure to close IGMP? (y/n)[n]:y
  Command is being executed. Please wait...
  Command has been executed successfully
```


Copyright © Huawei Technologies Co., Ltd.

```
huawei(config-mvlan1000)#igmp match mode disable
  Command has been executed successfully
```

(Optional) Set the address range for the dynamic programs. If you need to limit the address range of dynamic programs, perform this operation. For example, set the address range of dynamic programs to 224.1.1.1-224.1.1.100.

```
huawei(config-mvlan1000)#igmp match group ip 224.1.1.1 to-ip 224.1.1.100
```

9. Set the IGMP mode.

   Select the IGMP proxy mode.

   ```
   huawei(config-mvlan1000)#igmp mode proxy
     Are you sure to change IGMP mode? (y/n)[n]:y
     Command is being executed. Please wait...
     Command has been executed successfully
   ```

10. Configure the IGMP upstream port.

    Set the IGMP upstream port ID to 0/19/0 and working mode to **default**. Protocol packets are transmitted to all the IGMP upstream ports in the multicast VLAN.

    ```
    huawei(config-mvlan1000)#igmp uplink-port 0/19/0
    huawei(config-mvlan1000)#btv
    huawei(config-btv)#igmp uplink-port-mode default
    Are you sure to change the uplink port mode?(y/n)[n]:y
    ```

11. (Optional) Set multicast global parameters.

    In this example, the default settings are used for all the multicast global parameters.

12. Configure multicast users.

    Add service ports 1 and 2 as multicast users.

    ```
    huawei(config-btv)#igmp user add service-port 1
    huawei(config-btv)#igmp user add service-port 2
    huawei(config-btv)#multicast-vlan 1000
    huawei(config-mvlan1000)#igmp multicast-vlan member service-port 1
    huawei(config-mvlan1000)#igmp multicast-vlan member service-port 2
    huawei(config-mvlan1000)#quit
    ```

13. Save the data.

    ```
    huawei(config)#save
    ```

- The ONT does not need to be configured.

----End

9.7.1.10 Configuring the VoD Service

The OLT is connected to the remote bridging ONT through a GPON port to provide users with the VoD service.

Prerequisites

- The OLT is connected to the BRAS and the program source.
- The VLAN of the LAN switch port connected to the OLT is the same as the upstream VLAN of the OLT.
- The ONT has been added to the OLT. For details, see **9.7.1.3 Adding an ONT to an OLT**.

Copyright © Huawei Technologies Co., Ltd.

Data Plan

Item	Data
ONT line profile	Profile name: ftth T-CONT ID: 4 GEM port ID: 13
Traffic profile	ID: 8 802.1p priority: 4 CIR: off (unlimited) Priority-based scheduling policy: local-setting
VLAN Plan	Single VLAN tag: ● SVLAN ID: 1100 ● VLAN type: smart ● VLAN attribute: common ● CVLAN=SVLAN VLAN translation policy: ● ONT: adds CVLAN tags to iTV service packets. ● OLT: transparently transmits packets with SVLANs.

Procedure

Step 1 Configure the OLT.

1. Configure a traffic profile.

   Configure traffic profile 8. Set the CIR to off (unlimited), priority to 4, and priority-based scheduling policy to local-setting (that is, queues are scheduled based on the priority specified in the profile).

   NOTE

   Run the **display traffic table ip** command to query the existing traffic profiles in the system. If the existing traffic profiles in the system do not meet the requirements, run the **traffic table ip** command to add a traffic profile.

   ```
   huawei(config)#traffic table ip index 8 cir off priority 4 priority-policy
   local-setting
   ```

2. Configure the mapping relationship between a GEM port and a VLAN.

   The service flow of user VLAN 1100 is mapped to GEM port 13 in the ONT line profile.

   ```
   huawei(config)#ont-lineprofile gpon profile-name ftth
   huawei(config-gpon-lineprofile-1)#gem mapping 13 4 vlan 1100
   huawei(config-gpon-lineprofile-1)#commit
   huawei(config-gpon-lineprofile-1)#quit
   ```

3. Configure the VLAN of the Ethernet port on the ONT.

   If the ONT is connected to the STB through Ethernet port 2, add Ethernet port 2 to VLAN 1100.

Copyright © Huawei Technologies Co., Ltd.

```
huawei(config)#ont-srvprofile gpon profile-name ftth
huawei(config-gpon-srvprofile-1)#port vlan eth 2 1100
huawei(config-gpon-srvprofile-1)#commit
huawei(config-gpon-srvprofile-1)#quit
```

4. Configure the native VLAN of the ONT port.

   If the ONT is connected to the STB through Ethernet port 2, the native VLAN ID is 1100.

```
huawei(config-if-gpon-0/1)#ont port native-vlan 0 1 eth 2 vlan 1100
huawei(config-if-gpon-0/1)#ont port native-vlan 0 2 eth 2 vlan 1100
huawei(config-if-gpon-0/1)#quit
```

5. Create a service VLAN and add an upstream port to it.

   Add upstream port 0/19/0 to VLAN 1100.

```
huawei(config)#vlan 1100 smart
huawei(config)#port vlan 1100 0/19 0
```

6. Create service flows.

   Set the service VLAN to 1100, GEM port ID to 13, and VLAN translation mode to transparent transmission, and use traffic profile 8.

```
huawei(config)#service-port 3 vlan 1100 gpon 0/1/0 ont 1 gemport 13
rx-cttr 8 tx-cttr 8 tag-transform transparent
huawei(config)#service-port 4 vlan 1100 gpon 0/1/0 ont 2 gemport 13
rx-cttr 8 tx-cttr 8 tag-transform transparent
```

7. Save the data.

```
huawei(config)#save
```

Step 2 The ONT does not need to be configured.

----End

9.7.1.11 Configuring Link Aggregation, Congestion Control, and Security Policies

The global configuration of link aggregation and queue scheduling based on priorities ensures service reliability. The global configuration of security policies ensures service security.

Context

Link aggregation provides a higher bandwidth and uplink reliability for optical line terminals (OLTs) by aggregating multiple uplink Ethernet ports to one link aggregation group (LAG). Link aggregation is recommended.

Congestion control places the packets to be sent from a port into multiple queues that are marked with different priorities. Then, the packets are sent based on queue priorities. Congestion control is recommended.

Security policies ensure system, user, and service security.

NOTE

Enable a service security function based on the service type. For details, see **9.6.6 Principle of Security Data Plan**.

Procedure

- Configure link aggregation.

  The following configurations are used as an example to configure link aggregation:

Copyright © Huawei Technologies Co., Ltd.

- Uplink ports 0/19/0 and 0/19/1 are added to a LAG.
- The two ports send packets upstream based on the packets' source MAC addresses.
- The LAG works in Link Aggregation Control Protocol (LACP) static aggregation mode.

```
huawei(config)#link-aggregation 0/19 0-1 ingress workmode lacp-static
```

- Configure queue scheduling.

  According to quality of service (QoS) planning principles, all packets are scheduled in strict priority (SP) mode and mapped to queues according to the packets' priorities. For details about QoS planning principles, see **11.2.2 Principle of QoS Data Plan**.

```
huawei(config)#queue-scheduler strict-priority
huawei(config)#cos-queue-map cos0 0 cos4 4 cos5 5 cos6 6
```

- Configure system security.
  - Enable deny of service (DoS) anti-attack on the OLT.
    1. Run the **security anti-dos enable** command to globally enable DoS anti-attack.
    2. Run the **security anti-dos control-packet policy** command to configure a protocol packet processing policy that will be used when a DoS attack occurs.
    3. Run the **security anti-dos control-packet rate** command to configure the threshold for the rate of sending protocol packets to the CPU.
  - Enable IP address anti-attack on the OLT.

    Run the **security anti-ipattack enable** command to enable IP address anti-attack.
- Configure user security.
  - Enable MAC address anti-flapping on the OLT.

    Run the **security anti-macduplicate enable** command to enable MAC address anti-flapping.
  - Enable MAC address anti-spoofing on the OLT.
    1. In global config mode, run the **security anti-macspoofing enable** command to globally enable MAC address anti-spoofing.
    2. Enable MAC address anti-spoofing at VLAN level in global config mode or service profile mode:
       a. In global config mode, run the **security anti-macspoofing vlan** command to enable MAC address anti-spoofing.
       b. In global config mode, run the **vlan service-profile** command to create a VLAN service profile.
       c. Perform the following operations to enable MAC address anti-spoofing in VLAN service profile mode:
          a. Run the **security anti-macspoofing enable** command to enable MAC address anti-spoofing at VLAN level.
          b. Run the **commit** command to make the profile configuration take effect.
          c. Run the **quit** command to quit the VLAN service profile mode.
          d. Run the **vlan bind service-profile** command to bind the created VLAN service profile to a VLAN.
    3. (Optional) Run the **security anti-macspoofing max-mac-count** command to set the maximum number of MAC addresses that can be bound to a service flow.

Copyright © Huawei Technologies Co., Ltd.

4. (Optional) Run the **security anti-macspoofing exclude** command to configure the types of packets for which MAC address anti-spoofing does not take effect, such as Internet Group Management Protocol (IGMP) packets.

- Enable IP address anti-spoofing on the OLT.

  IP address anti-spoofing can be enabled or disabled at three levels: global, VLAN, and service port levels. This function takes effect only after it is enabled at the three levels. Among the three levels, IP address anti-spoofing is disabled only at the global level by default.

  1. In global config mode, run the **security anti-ipspoofing enable** command to enable IP address anti-spoofing at the global level.
  2. In VLAN service profile mode, run the **security anti-ipspoofing enable** command to enable IP address anti-spoofing at the VLAN level.
  3. Run the **security anti-ipspoofing service-port** *serviceport-id* **enable** command to enable IP address anti-spoofing at the service port level.

- Configure service security.
  - Enable Dynamic Host Configuration Protocol (DHCP) Option 82 on the OLT. This configuration is recommended for the DHCP-based Internet access service.

    1. Enable DHCP Option 82 on the OLT.

       DHCP Option 82 can be enabled or disabled at four levels: global, port, VLAN, and service port levels. This function takes effect only after it is enabled at the four levels. Among the four levels, DHCP Option 82 is disabled only at the global level by default.

       - The global level: In global config mode, run the **dhcp option82** command to enable DHCP Option 82 at the global level.

         When you run this command, select the **enable**, **forward**, or **rebuild** parameter based on site requirements. The three parameters can all enable DHCP Option 82 but provide different packet processing policies on the OLT. For details, see the **dhcp option82** command.
       - The port level: In global config mode, run the **dhcp option82 port** or **dhcp option82 board** command to enable DHCP Option 82 at the port level.
       - The VLAN level:

         a. In global config mode, run the **vlan service-profile** command to create a VLAN service profile.
         b. Run the **dhcp option82 enable** command to enable DHCP Option 82 at the VLAN level.
         c. Run the **commit** command to make the profile configuration take effect.
         d. Run the **quit** command to quit the VLAN service profile mode.
         e. Run the **vlan bind service-profile** command to bind the created VLAN service profile to a VLAN.
       - The service port level: In global config mode, run the **dhcp option82 service-port** command to enable DHCP Option 82 at the service port level.

    2. On the OLT, run the **dhcp-option82 permit-forwarding service-port** command with the **enable** parameter selected, to allow ONT DHCP packets to carry Option 82 information.

Copyright © Huawei Technologies Co., Ltd.

- Enable Policy Information Transfer Protocol (PITP) on the OLT. This configuration is recommended for the PPPoE-based Internet access service.

  1. Enable PITP on the OLT.

     PITP can be enabled or disabled at four levels: global, port, VLAN, and service port levels. This function takes effect only after it is enabled at the four levels. Among the four levels, PITP is disabled only at the global level by default.

     - The global level: In global config mode, run the **pitp enable pmode**, **pitp forward pmode**, or **pitp rebuild pmode** command to enable PITP at the global level.

       In the preceding commands, the **enable**, **forward**, and **rebuild** parameters can all enable PITP but provide different packet processing policies on the OLT. Select one of them based on site requirements. For details, see the **pitp** command.
     - The port level: In global config mode, run the **pitp port** or **pitp board** command to enable PITP at the port level.
     - The VLAN level:

       a. In global config mode, run the **vlan service-profile** command to create a VLAN service profile.

       b. Run the **pitp enable** command to enable PITP at the VLAN level.

       c. Run the **commit** command to make the profile configuration take effect.

       d. Run the **quit** command to quit the VLAN service profile mode.

       e. Run the **vlan bind service-profile** command to bind the created VLAN service profile to a VLAN.
     - The service port level: In global config mode, run the **pitp service-port** command to enable PITP at the service port level.

  2. On the OLT, run the **pitp permit-forwarding service-port** command with the **enable** parameter selected, to allow ONT PPPoE packets to carry a vendor tag.

----End

9.7.1.12 Verifying Services

In the FTTH scenario, ONTs are installed in users' houses which are far away from the central equipment room. ONTs provide remote service verification methods including PPPoE dialup emulation, call emulation, and multicast emulation to facilitate configuration and commissioning engineers to verify services remotely after service configuration.

Prerequisites

ONTs and upper-layer devices have been connected properly. The BRAS and MGC/IMS have been configured.

Copyright © Huawei Technologies Co., Ltd.

Background

Remote Service Verification Method	Function	Description
PPPoE dialup emulation	An ONT simulates a PPPoE user terminal software to perform dialup and interact with the BRAS to verify the connectivity between the ONT and BRAS.	● PPPoE dialup emulation requires a service flow which does not belong to a QinQ VLAN. ● A user name, password, and authentication mode must be configured on the BRAS for the PPPoE dialup emulation. ● An ONT supports a maximum of a PPPoE dialup emulation.
Call Emulation	An ONT simulates a voice user to make a call to check whether the voice service data is correctly configured. You can also use the call emulation function to locate a fault when the voice service is faulty.	● An ONT can simulate a caller or callee to communicate with a phone in a call. In this case, only a functional phone is required in the central office where the acceptance personnel is. ● An ONT supports a maximum of a call emulation.
Multicast emulation	This function enables you to simulate a multicast user going online and lead the program stream to an ONT. You can check whether the multicast service is normal by checking the real-time traffic of the multicast program.	Multicast services configured in the dynamic controllable multicast mode do not support this function.

Data plan

Item	Data	Remarks
PPPoE dialup emulation parameters	PPPoE user name: test@huawei Password: test	The user name, password, and authentication mode for the emulation test must be configured on the BRAS. The entered user name, password, and authentication mode must be consistent with those configured on the BRAS.
Call emulation parameters	ONT POTS ID: 1	The default values are used. You can run the **display pots emulational configuration** command to check the parameter values.

Copyright © Huawei Technologies Co., Ltd.

Item	Data	Remarks
Multicast emulation parameters	Multicast service flow ID: 1 MVLAN: 1000 IP address of the multicast program: 224.1.1.10	-

Procedure

- Verify the Internet access service using PPPoE dialup emulation.
  1. In the xPON board mode, run the **pppoe simulate start** command to start a PPPoE dialup emulation test. The following test uses GPON as an example:

```
huawei(config)#interface gpon 0/1
huawei(config-if-gpon-0/1)#pppoe simulate start
{ portid<U><0,7> }:0
{ ontid<U><0,127> }:1
{ eth<K>|untagged<K>|vlanid<U><0,4095> }:eth
{ ont-portid<U><1,8> }:4
{ untagged<K>|vlanid<U><0,4095> }:100
{ priority<U><0,7>|user-name<K> }:user-name
{ username<S><Length 1-64> }:test@huawei
{ user-password<K> }:user-password
{ password<S><Length 1-64> }:test
{ authentication-mode<K> }:authentication-mode
{ protocol<E><chap,pap> }:chap

  Command:
          pppoe simulate start 0 1 eth 4 100 user-name test@huawei user-
password
 test authentication-mode chap

huawei(config-if-gpon-0/1)#
  ---------------------------------
  ONT PPPoE Test Result
  ---------------------------------
  F/S/P                : 0/1/0
  ONT-ID               : 1
  ONT ETH Port ID      : 4
  ONT Vlan ID          : 100
  Vlan Priority        : -
  Emluator result      : Success
  Session ID           : 18814
  User IP              : 192.168.100.101
  Gateway IP           : 192.168.100.1
  ---------------------------------
```

- Troubleshooting methods for the Internet access service
  1. Check whether configurations are complete on the OLT.
     - Run the **display ont info** command to query the ONT status to check whether the ONT is registered successfully.
     - Run the **display service-port** command to check whether the Internet access service flow is configured and whether the inner VLAN ID of the service flow is consistent with that in the data plan.

Copyright © Huawei Technologies Co., Ltd.

- If a native VLAN is configured for the Ethernet port on the ONT, run the **display ont port attribute** command in the xPON board mode to check whether the native VLAN is correct.

2. Check the upstream and downstream ports by checking the MAC address learning status.

   a. Run the **display mac-address vlan** command to check the MAC address learning status of the Internet service VLAN.

      - If the upstream port does not learn a MAC address, check the network connections between the upstream port and upper-layer devices and check the configurations of upper-layer devices.
      - If the downstream port does not learn a MAC address, check whether the ONT is activated, whether the PC is connected to the right port on the ONT, and whether the PC is working properly.

   b. Run the **display ont-learned-mac** command to check whether the ONT connecting to the PON port learned any MAC addresses.

      If not, check whether the ONT properly connects to the PC or home gateway (HGW).

- Verify the voice service using call emulation.

  1. Run the **ont emulational call** command to configure a call emulation test.

```
huawei(config)#test
huawei(config-test)#ont emulational call caller-port 0/1/0 1 1 telno
77730020
{ <cr>|caller-stop-time<K> }:

  Command:
          ont emulational call caller-port 0/1/0 1 1 telno 77730020
```

  2. The ONT outputs the call emulation result after the test is complete.

```
huawei(config-test)#
  ------------------------------------------------------------------
  F/S/P                : 0/1/0
  ONT-ID               : 0
  ONT-POTSID           : 1
  Test type            : caller emulational call test
  Detected number      : 77730020
  Reported number      : 77730020
  Current status       : test end
  Test Result          : success
  ------------------------------------------------------------------
```

- Troubleshooting methods for the voice service.

  1. Check whether configurations are complete on the OLT.

     - Run the **display ont info** command to query the ONT status to check whether the ONT is registered successfully.
     - Run the **display service-port** command to check whether the voice service flow is configured and whether the inner VLAN ID of the service flow is consistent with that in the data plan.

  2. Check the upstream and downstream ports by checking the MAC address learning status.

     Run the **display mac-address vlan** command to check the MAC address learning status of the voice service VLAN.

Copyright © Huawei Technologies Co., Ltd.

- If the upstream port does not learn a MAC address, check the network connections between the upstream port and upper-layer devices and check the configurations of upper-layer devices.
- If the downstream port does not learn a MAC address, check whether the ONT is activated and whether physical links are normal.
- If both the upstream and downstream ports can learn the MAC address, record the MAC address of the ONT and log in to the service router (SR) to check whether an IP address is allocated to the MAC address.

3. Check the registration status of the voice service.
   - You can run the **display ont port state** command on the OLT to query the call connection status on the POTS port. If **Call State** is **RegisterFail** or **Connecting** for a long time, check whether the voice configuration on the MGC/SIP server is consistent with that on the ONT.
   - If the ONT uses the H.248 protocol, you can run the **display ont mg status** command on the OLT to query the registration status of the MG interface that connects to the ONT. If **MG Status** is **UnRegistered** or **Registering** for a long time, check whether the voice configuration on the MGC/SIP server is consistent with that on the ONT.
   - You can query the registration status of the voice service on the ONT web page. If the query result shows that the registration fails or the voice service is in the registering state for a long time, check whether the voice configuration on the MGC/SIP server is consistent with that on the ONT.

- Verify the multicast service using multicast emulation.
  1. Run the **igmp static-join** command to simulate a multicast user to order a multicast program.

     ```
     huawei(config)#btv
     huawei(config-btv)#igmp static-join service-port 1 ip 224.1.1.10 vlan 1000
     ```

     NOTE

     If the multicast program is obtained dynamically, **igmp static-join** can be executed successfully only when the range for obtaining the dynamic program is set.

  2. Run the **display igmp user** command to query the status of the multicast user.

     ```
     huawei(config-btv)#display igmp user service-port 1
       User                       : 0/1/0/1
       State                      : online
       Authentication             : no-auth
       Quick leave                : MAC-based
       IGMP flow ID               : 1
       Video flow ID              : 1
       Log switch                 : enable
       Bind profiles              : -
       IGMP version               : IGMP v3
       Current version            : IGMP v3
       Current IGMP IPv6 version  : IGMP IPv6 v2
       Available programs         : 8
       Global leave               : disable
       User max bandwidth         : no-limit
       Used bandwidth(kbps)       : 0
       Used bandwidth
       to max bandwidth(%)        : -
       Total video bandwidth      : -
       Mcast video bandwidth      : -
       Active program list

       ------------------------------------------------------------------------
     ```


Copyright © Huawei Technologies Co., Ltd.

```
--
  Program name     VLAN  IP/MAC          State           Start time

-------------------------------------------------------------------------
--
  PROGRAM-5        1000  224.1.1.10      watching        2011-10-29
                                                        16:33:41+08:00

-------------------------------------------------------------------------
--
  Total: 1
```

3. Run the **display multicast flow-statistic** command to query the real-time traffic of the multicast program.

```
huawei(config-btv)#display multicast flow-statistic vlan 1000 ip
224.1.1.10
{ <cr>|sourceip<K> }:

  Command:
          display multicast flow-statistic vlan 1000 ip 224.1.1.10
  Command is being executed. Please wait...
  Multicast flow statistic result: 8736(kbps)
```

----End

9.7.2 Bridging ONT + HGW Network Scenario

This topic describes how to configure Internet access service, voice service, BTV service and VoD service when bridging ONTs + HGWs are used to build an FTTH network.

9.7.2.1 Service Requirements and Application Scenario

Service Requirements

Optical fibers are connected to user homes and triple play services are required. The following provides detailed service requirements:

- Internet access of multiple PCs in a home is supported.
- Access of multiple telephones in a home is supported.
- IPTV programs can be previewed and watched using STBs.
- Service extension is supported and different services do not affect each other.
- Proper service security is ensured.
  - Internet access services are protected against unauthorized access, user account theft or borrowing, MAC/IP spoofing, and malicious attacks.
  - Voice and IPTV services are protected against MAC/IP spoofing, malicious attack, and traffic flooding attacks.
- Service faults are easy to locate and services are easy to maintain.

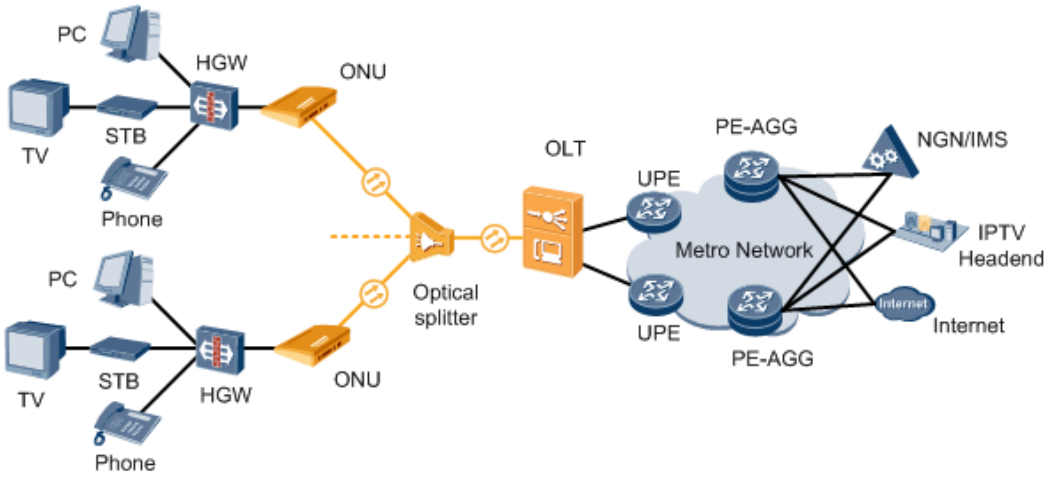
Application Scenario

As shown in **Figure 9-3**, the HGW integrating an IAD provides Internet, voice over Internet Protocol (VoIP), and Internet Protocol television (IPTV) services to users.

Services are mainly implemented on the HGW, and the bridging ONT works with the OLT to provide Layer 2 channels.

Copyright © Huawei Technologies Co., Ltd.

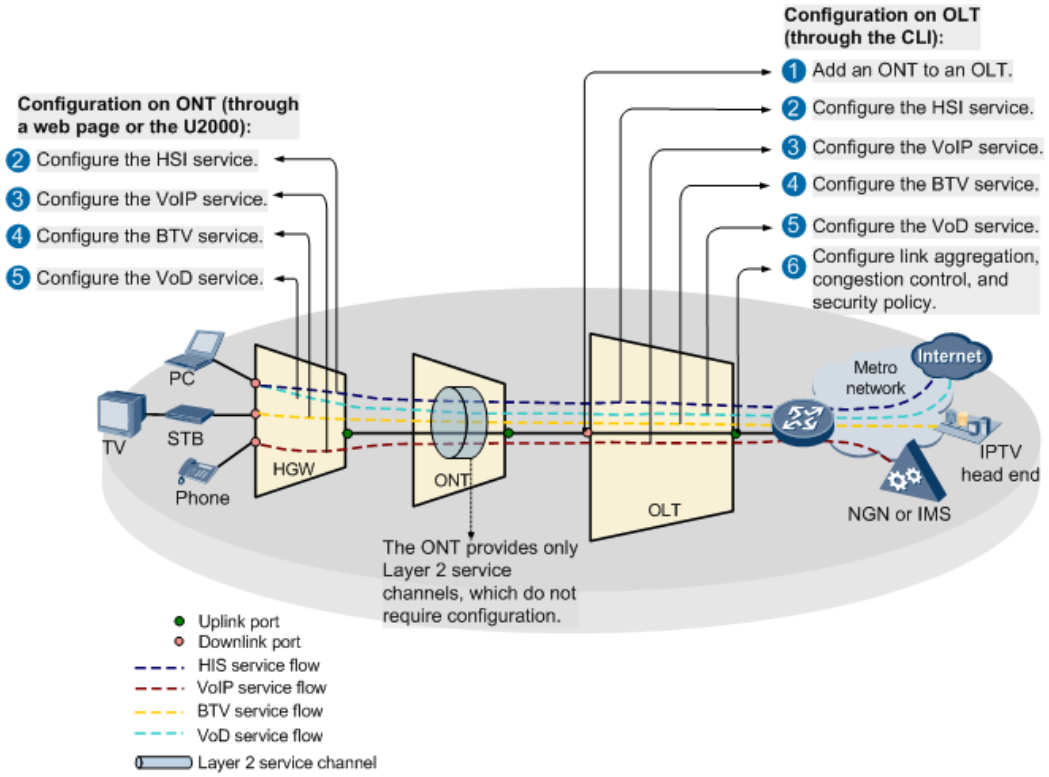
Figure 9-3 Bridging ONT + HGW



9.7.2.2 Configuration Process

Figure 9-4 shows the configuration roadmap in fiber to the home (FTTH) networking using a bridging optical network terminal (ONT)+home gateway (HGW).

Figure 9-4 Configuration roadmap in FTTH networking using a bridging ONT+HGW



The following table describes the configuration steps.

Copyright © Huawei Technologies Co., Ltd.

Item	Step		Description
Optical line terminal (OLT)	**9.7.1.3 Adding an ONT to an OLT**		Services can be configured for an ONT only after the ONT is successfully added to an OLT.
OLT HGW	**9.7.2.4 Configuring the Internet Access Service**		● An ONT provides only Layer 2 service channels, which do not require configuration. An HGW is equipped with an integrated access device (IAD) provides the Internet access, VoIP, and IPTV services for users. ● IPTV services include the BTV and VoD services that are different in configuration procedures and need to be configured separately.
	9.7.2.5 Configuring the Voice Service		
	Configure the IPTV service.	**9.7.2.6 Configuring the BTV Service**	
		9.7.2.7 Configuring the VoD Service	
OLT	**9.7.1.11 Configuring Link Aggregation, Congestion Control, and Security Policies**		The global configuration of link aggregation and queue scheduling based on priorities ensures service reliability. The global configuration of security policies ensures service security.
OLT	**9.7.1.12 Verifying Services**		The OLT provides remote verification methods including ONT PPPoE/DHCP dialup emulation and call emulation for configuration and commissioning engineers to verify services remotely after service configuration, avoiding a second on-site operation.

9.7.2.3 Adding an ONT to an OLT

Services can be configured for an ONT only after the ONT is successfully added to an OLT.

Copyright © Huawei Technologies Co., Ltd.

Data Plan

Table 9-4 Data plan

Item	Data
DBA profile	Profile name: ftth_dba Profile type: type3 Assured bandwidth: 8 Mbit/s Maximum bandwidth: 20 Mbit/s
ONT line profile	Profile name: ftth T-CONT ID: 4 GEM port ID for management services: 11 GEM port ID for voice services: 12 GEM port ID for video services: 13 GEM port ID for Internet access services: 14
ONT service profile	Profile name: ftth ONT port capability set: adaptive
Network topology data	PON port: 0/1/0 ONT IDs: 1 and 2

Procedure

Step 1 Configure GPON ONT profiles.

GPON ONT profiles include the DBA profile, line profile, service profile, and alarm profile.

- DBA profile: A DBA profile describes GPON traffic parameters. A T-CONT is bound to a DBA profile for dynamic bandwidth allocation, improving upstream bandwidth utilization.
- Line profile: A line profile describes the binding between the T-CONT and the DBA profile, the QoS mode of the traffic stream, and the mapping between the GEM port and the ONT-side service.
- Service profile: A service profile provides the service configuration channel for the ONT that is managed by using optical network terminal management and control interface (OMCI).
- Alarm profile: An alarm profile contains a series of alarm thresholds to measure and monitor the performance of activated ONT lines. When a statistical value reaches the threshold, the host is notified and an alarm is reported to the log host and the NMS.

1. Configure a DBA profile.

   Run the **display dba-profile** command to query existing DBA profiles in the system. If the existing DBA profiles in the system do not meet the requirements, run the **dba-profile add** command to add a DBA profile.

Copyright © Huawei Technologies Co., Ltd.

Create the same DBA profile for different types of services. Set the profile name to **ftth_dba**, profile type to **type3**, assured bandwidth to 8 Mbit/s, and maximum bandwidth to 20 Mbit/s.

```
huawei(config)#dba-profile add profile-name ftth_dba type3 assure 8192 max
20480
```

NOTE

The DBA implementation is based on an ONT. Therefore, select a DBA profile of the proper bandwidth type and configure proper bandwidth according to the service types and total user count of the ONT. Note that the sum of the fixed bandwidth and the assured bandwidth must not be greater than the total bandwidth of the PON port.

2. Configure an ONT line profile.

   Create a GPON ONT line profile, named **ftth**, and bind it to the DBA profile **ftth_dba**.

   ```
   huawei(config)#ont-lineprofile gpon profile-name ftth
   huawei(config-gpon-lineprofile-1)#tcont 4 dba-profile-name ftth_dba
   ```

   Create different GEM ports according to different service types, in which

   - GEM port 11 is used to carry management services.
   - GEM port 12 is used to carry voice services.
   - GEM port 13 is used to carry video services.
   - GEM port 14 is used to carry Internet access services.

   ```
   huawei(config-gpon-lineprofile-1)#gem add 11 eth tcont 4
   huawei(config-gpon-lineprofile-1)#gem add 12 eth tcont 4
   huawei(config-gpon-lineprofile-1)#gem add 13 eth tcont 4
   huawei(config-gpon-lineprofile-1)#gem add 14 eth tcont 4
   ```

   NOTE

   1. To change the default QoS mode, run the **qos-mode** command to set the QoS mode to **gem-car** or **flow-car**, and run the **gem add** command to set the index of the traffic profile bound to the GEM port.
   2. When the QoS mode is priority-queue (PQ), the default queue priority is 0; when the QoS mode is flow-car or gem-car, traffic profile 6 is bound to the GEM port by default (no rate limitation).

   After the configurations are complete, run the **commit** command to apply the parameters settings.

   ```
   huawei(config-gpon-lineprofile-1)#commit
   huawei(config-gpon-lineprofile-1)#quit
   ```

3. Configure an ONT service profile.

   Create a GPON ONT service profile, named **ftth**. Configure the capability set of the ETH port and POTS port to **adaptive**. Then the system automatically adapts to the ONT according to the actual capability of the online ONT.

   ```
   huawei(config)#ont-srvprofile gpon profile-name ftth
   huawei(config-gpon-srvprofile-1)#ont-port eth adaptive pots adaptive
   ```

   After the configurations are complete, run the **commit** command to apply the parameters setting.

   ```
   huawei(config-gpon-srvprofile-1)#commit
   huawei(config-gpon-srvprofile-1)#quit
   ```

4. (Optional) Add an alarm profile.

   - The default GPON alarm profile 1 is used. The alarm thresholds of the default alarm profile are 0, which indicates that no alarm is generated.
   - In this example, the default alarm profile is used, and therefore the configuration of the alarm profile is not required.

Copyright © Huawei Technologies Co., Ltd.

- Run the **gpon alarm-profile add** command to configure a GPON alarm profile, which is used for monitoring the performance of an activated ONT line.

Step 2 Add an ONT.

Connect two ONTs to GPON port 0/1/0. Set the ONT IDs to **1** and **2**, SNs to **32303131D659FD40** and **6877687714852901**, passwords to **0100000001** and **0100000002**, discovery mode for password authentication to **once-on**, and management mode to **OMCI**. Bind the two ONTs to ONT line profile **ftth** and ONT service profile **ftth**.

There are two methods of adding an ONT: add an ONT offline and confirm an automatically discovered ONT.

- Add ONTs offline.

  If the password of an ONT is known, run the **ont add** command to add an ONT offline.

```
huawei(config)#interface gpon 0/1
huawei(config-if-gpon-0/1)#ont add 0 1 password-auth 0100000001 once-on no-aging
omci ont-lineprofile-name
 ftth ont-srvprofile-name ftth
huawei(config-if-gpon-0/1)#ont add 0 2 password-auth 0100000002 once-on no-aging
omci ont-lineprofile-name
 ftth ont-srvprofile-name ftth
```

- Confirm automatically discovered ONTs.

  If the password or SN of an ONT is unknown, run the **port** ***portid*** **ont-auto-find** command in GPON mode to enable the ONT auto-discovery function of the GPON port. Then, run the **ont confirm** command to confirm the ONT.

```
huawei(config)#interface gpon 0/1
huawei(config-if-gpon-0/1)#port 0 ont-auto-find enable
huawei(config-if-gpon-0/1)#display ont autofind 0
  //After this command is executed, the information about all ONTs connected to
the GPON port through optical splitters is displayed.

huawei(config-if-gpon-0/1)#ont confirm 0 ontid 1 sn-auth 32303131D659FD40 omci
ont-lineprofile-name
 ftth ont-srvprofile-name ftth
huawei(config-if-gpon-0/1)#ont confirm 0 ontid 2 sn-auth 6877687714852901 omci
ont-lineprofile-name
 ftth ont-srvprofile-name ftth
```

  NOTE

  If multiple ONTs of the same type bound to the same line profile or service profile are connected to the same port, you can bulk add ONTs by bulk confirming automatically discovered ONTs to make configuration easier and more efficient. To do so, the preceding command can be modified as follows:

```
huawei(config-if-gpon-0/1)#ont confirm 0 all sn-auth omci ont-lineprofile-name
ftth
ont-srvprofile-name ftth
```

- (Optional) Bind the alarm profile to the ONT.

  The default profile 1 is used in this example.

```
huawei(config-if-gpon-0/1)#ont alarm-profile 0 1 profile-id 1
huawei(config-if-gpon-0/1)#ont alarm-profile 0 2 profile-id 1
```

Step 3 Check ONT status.

After an ONT is added, run the **display ont info** command to query the current status of the ONT. Ensure that **Config flag** of the ONT is **active**, **Run State** is **online**, **Config state** is **normal**, and **Match state** is **match**.

```
huawei(config-if-gpon-0/1)#display ont info 0 1
  ------------------------------------------------------------------------
```


Copyright © Huawei Technologies Co., Ltd.

```
  F/S/P                : 0/1/0
  ONT-ID               : 1
  Control flag         : active    //Indicates that the ONT is
activated.
  Run state            : online    //Indicates that the ONT goes online
successfully.
  Config state         : normal    //Indicates that the configuration state of the
ONT is normal.
  Match state          : match     //Indicates that the capability profile bound to
the ONT is consistent with the actual capability of the ONT.
...//The rest of the response information is omitted.
```

When **Config state** is **failed**, **Run state** is **offline**, or **Match state** is **mismatch**:

- If **Control flag** is **deactive**, run the **ont active** command in GPON mode to activate the ONU.
- If **Run state** is **offline**, a physical line may be broken or the optical module may be damaged. Check the line and the optical module.
- If **Config state** is **failed**, the configured ONU capability exceeds the actual ONU capability. In this case, run the **display ont failed-configuration** command in the diagnose mode to check the failed configuration item and the failure cause. Then, rectify the fault accordingly.
- If the ONU does not match, that is, **Match state** is **mismatch**, the port types and number of ports undermatch the actual port types and number of ports supported by the ONU. In this case, run the **display ont capability** command to query the actual capability of the ONU, and then select one of the following modes to modify the ONU configuration:
  - Create a proper ONU profile according to the actual capability of the ONU, and then run the **ont modify** command to modify the configuration data of the ONU.
  - Modify the ONU profile according to the actual capability of the ONU and save the modification. Then, the ONU automatically recovers the configuration successfully.

----End

9.7.2.4 Configuring the Internet Access Service

The OLT is connected to the remote ONT through a GPON port to provide users with high-speed Internet access services.

Prerequisites

- The OLT is connected to the BRAS.
- Related configurations are performed on the BRAS according to the authentication and accounting requirements for dialup users. For details about the configuration, see the configuration guide.
- The ONT has been added to the OLT. For details, see **9.7.1.3 Adding an ONT to an OLT**.
- The VLAN of the LAN switch port connected to the OLT is consistent with the upstream VLAN of the OLT.
- Residential users generally access the Internet in Point-to-Point Protocol over Ethernet (PPPoE) dial-up mode. PPPoE dial-up can be performed on personal computers (PCs) or HGWs.
- The configuration processes on HGWs of different models or in different appearances are similar. This topic describes how to configure the Internet access service on an HG239 that is connected to an ONT upstream through a LAN.

Copyright © Huawei Technologies Co., Ltd.

Data Plan

Item	Data
ONT line profile	Profile name: ftth T-CONT ID: 4 GEM port ID for Internet access service: 14
Network topology data	Upstream port: 0/19/0 PON port: 0/1/0 ONT IDs: 1 and 2 ID of the port on the HGW that is connected to the PC: 1
VLAN Plan	Double-tagged VLAN: ● S-VLAN ID: 100 ● S-VLAN type: smart ● S-VLAN attribute: stacking ● C-VLAN ID: 1001-1002 ● U-VLAN ID: 45 VLAN translation policy: ● ONT: The upstream packets sent from the HGW carry user-VLANs and the ONT transparently transmits them. ● OLT: The OLT translates the U-VLAN to S-VLAN+C-VLAN.

Procedure

- Configure the OLT.
  1. Configure a traffic profile.

     Run the **display traffic table ip** command to query existing traffic profiles in the system. If the traffic profiles existing in the system do not meet the requirements, you need to run the **traffic table ip** command to add a traffic profile.

     Set the profile ID to ftth_hsi, the CIR to 4 Mbit/s, and the priority to 0. In addition, configure the scheduling mode so that packets are scheduled according to their priorities.

     ```
     huawei(config)#traffic table ip name ftth_hsi cir 4096 priority 0 priority-policy local-setting
     ```

  2. Configure the mapping between a GEM port and a VLAN.

     The service flow of user-side VLAN 45 is mapped to GEM port 14 in the ONT line profile.

     NOTE

     Here, the user-side VLAN is the VLAN carried by packets sent from HGW to ONT, namely, U-VLAN.

     ```
     huawei(config)#ont-lineprofile gpon profile-name ftth
     huawei(config-gpon-lineprofile-1)#gem mapping 14 0 vlan 45
     ```


Copyright © Huawei Technologies Co., Ltd.

```
huawei(config-gpon-lineprofile-1)#commit
huawei(config-gpon-lineprofile-1)#quit
```

3. Configure the VLAN of the Ethernet port on the ONT.

   Add Ethernet port 1 to VLAN 45 in the ONT service profile.

```
huawei(config)#ont-srvprofile gpon profile-name ftth
huawei(config-gpon-srvprofile-1)#port vlan eth 1 45
huawei(config-gpon-srvprofile-1)#commit
```

4. Create an Internet access service VLAN and add an upstream port to it.

   Add upstream port 0/19/0 to VLAN 100.

```
huawei(config)#vlan 100 smart
huawei(config)#vlan attrib 100 stacking
huawei(config)#port vlan 100 0/19 0
```

5. Create Internet access service flows.

   Set S-VLAN ID to 100 and GEM port ID to 14. Use traffic profile ftth_hsi.

```
huawei(config)#service-port vlan 100 gpon 0/1/0 ont 1 gemport 14 multi-
service
user-vlan 45 tag-transform translate-and-add inner-vlan 1001 inbound
traffic-table
 name ftth_hsi outbound traffic-table name ftth_hsi
huawei(config)#service-port vlan 100 gpon 0/1/0 ont 2 gemport 14 multi-
service
user-vlan 45 tag-transform translate-and-add inner-vlan 1002 inbound
traffic-table
name ftth_hsi outbound traffic-table name ftth_hsi
```

6. Save the data.

```
huawei(config)#save
```

- Configure the HGW.
  1. Log in to the Web configuration window.
     a. Enter http://192.168.1.1/cu.html (default IP address) to the address bar of the Internet Explorer (IE) and press Enter.
     b. In the login dialog box, enter the user name and password of the administrator (the Internet service provider (ISP) provides the default user name and default password). Then, click **OK**.
  2. Set parameters for the Internet access service.

     Assume that ports LAN1 and LAN2 are Internet access ports for PCs.
     a. Choose **Network** > **Bandwidth Configuration** from the navigation tree.
     b. Create WAN connection 1 and set parameters based on the following table.

Parameter	Value
Bearing service	INTERNET

Copyright © Huawei Technologies Co., Ltd.

Parameter	Value
VLAN enabling	Enabled: Upstream packets contain VLAN tags. Disabled: Upstream packets do not contain VLAN tags. **NOTE** If **uservlan** is set to **untagged** when you configure a service flow for the Internet access service on the OLT, set this parameter to **Disabled**; otherwise, set it to **Enabled**.
VLANID [1-4094]	If **VLAN enabling** is set to **Enabled**, this parameter takes the value of **uservlan** that is specified when you configure a service flow for the Internet access service on the OLT.
Binding item	LAN1 and LAN2: PCs connected to ports LAN1 and LAN2 can simultaneously access the Internet.
Mode	Bridge: PCs access the Internet in PPPoE dial-up mode.

c. Click **OK**.

3. Restart the HGW.

   Choose **Management** > **Device Management** and click **Restarting the Device**.

----End

9.7.2.5 Configuring the Voice Service

The OLT is connected to the remote ONT through a GPON port to provide users with the IP-based high-quality and low-cost VoIP service.

Prerequisites

- The SIP interface data and POTS user configuration data corresponding to the MG interface have been configured on the SIP server.
- The connection between the OLT and the SIP server is set up. The OLT can ping the IP address of the SIP server successfully.
- The ONT has been added to the OLT. For details, see **9.7.1.3 Adding an ONT to an OLT**.
- HGWs have different models and appearances but their configuration procedures are similar. This topic uses the HG255 that uses LAN for upstream transmission as examples.
- The IADs use SIP as the voice protocol.

Data Plan

Item	Data
ONT line profile	Profile name: ftth T-CONT ID: 4 GEM port ID: 12

Copyright © Huawei Technologies Co., Ltd.

Item	Data
VLAN plan	Single VLAN tag: ● VLAN ID: 300 ● VLAN type: smart ● VLAN attribute: common ● UVLAN ID: 47 VLAN translation policy: ● ONT: Packets that are sent upstream by the HGW are tagged with a user VLAN. The ONT transparently transmits the user VLAN. ● OLT: translates the VLAN tag (user VLAN <-> S-VLAN).
Voice parameter	IP address of the SIP server: 200.200.200.200/24 Port ID of the SIP server: 5060 User phone number: 77730010

Procedure

- Configure the OLT.
  1. Configure a traffic profile.

     Run the **display traffic table ip** command to query the existing traffic profiles in the system. If the existing traffic profiles in the system do not meet the requirements, run the **traffic table ip** command to add a traffic profile.

     Set the profile name to **ftth_voip** and do not limit the upstream and downstream rates. Set the priority to **5** and packets are scheduled according to the priority carried.

     ```
     huawei(config)#traffic table ip name ftth_voip cir off priority 5 priority-policy
      local-setting
     ```

  2. Configure the mapping relationship between a GEM port and a VLAN.

     The service flow of user VLAN 47 is mapped to GEM port 12 in the ONT line profile.

     NOTE

     The user VLAN is the VLAN in the packets sent from the HGW to the ONT, that is, the UVLAN.

     ```
     huawei(config)#ont-lineprofile gpon profile-name ftth
     huawei(config-gpon-lineprofile-1)#gem mapping 12 2 vlan 47
     huawei(config-gpon-lineprofile-1)#commit
     huawei(config-gpon-lineprofile-1)#quit
     ```

  3. Configure the VLAN of the Ethernet port on the ONT.

     If the ONT is connected to the HGW through Ethernet port 1, add Ethernet port 1 to VLAN 47 in the ONT service profile.

     ```
     huawei(config)#ont-srvprofile gpon profile-name ftth
     huawei(config-gpon-srvprofile-1)#port vlan eth 1 47
     ```


Copyright © Huawei Technologies Co., Ltd.

```
huawei(config-gpon-srvprofile-1)#commit
huawei(config-gpon-srvprofile-1)#quit
```

4. Create a service VLAN and add an upstream port to it.

   Add upstream port 0/19/0 to VLAN 300.

   ```
   huawei(config)#vlan 300 smart
   huawei(config)#port vlan 300 0/19 0
   ```

5. Create service flows.

   Set the service VLAN to 300, GEM port ID to 12, and user VLAN to 47, and use traffic profile **ftth_voip**.

   ```
   huawei(config)#service-port vlan 300 gpon 0/1/0 ont 1 gemport 12 multi-
   service
    user-vlan 47 inbound traffic-table name ftth_voip outbound traffic-table
   name
   ftth_voip
   huawei(config)#service-port vlan 300 gpon 0/1/0 ont 2 gemport 12 multi-
   service
    user-vlan 47 inbound traffic-table name ftth_voip outbound traffic-table
   name
   ftth_voip
   ```

6. Enable the ARP proxy function.

   Voice media streams for different users of the same SVLAN fail to interchange because the service ports of the smart VLAN are isolated from each other. Therefore, the ARP proxy function needs to be enabled on the OLT.

   ```
   huawei(config)#arp proxy enable
   huawei(config)#interface vlanif 300
   huawei(config-if-vlanif300)#arp proxy enable
   huawei(config-if-vlanif300)#quit
   ```

7. Save the data.

   ```
   huawei(config)#save
   ```

- Configure the HGW.

  1. Log in to the Web configuration interface.

     a. Enter **http://192.168.1.1** (default IP address) in the address bar of the browser and press Enter.

     b. In the login window, enter the user name and password (the default value is provided by ISP) of the administrator and click **OK**.

  2. Configure parameters of the voice service.

     The configuration procedure is as follows:

     a. In the Web page, choose **Network** > **Bandwidth Configuration** from the navigation tree.

     b. Create WAN Connection 2 for the VoIP service and set the parameters as follows:

Parameter	Value
Bearing service	VoIP
Enabling status	Enable

Copyright © Huawei Technologies Co., Ltd.

Parameter	Value
VLAN mode	VLAN Transparent Transmission
VLAN ID	VLAN ID corresponding to the user VLAN value for voice service flows created on the OLT. In this example, set this parameter to 47.
802.1p	Enabled
Mode	Route: route mode
DHCP	Enabled
NAT	Enabled

c. Click **OK** to save the settings.

d. Choose **Appliciation** > **Broadband Phone Configuration** from the navigation tree. Configure the parameters as follows:

Parameter	Value
Address	Preferred IP address of the proxy server: 200.200.200.200
Port ID	Preferred signaling port ID of the proxy server: 5060
Enabling	Enabled
User number	When logging in to a VoIP account, you can set the user account to the user telephone number. In this example, set the user telephone number to 77730010.
User password	-

3. Restart the HGW.

   Choose **Management** > **Device Management** and click **Restarting the Device**.

----End

9.7.2.6 Configuring the BTV Service

The OLT is connected to the remote bridging ONT through a GPON port to provide users with the multicast service.

Prerequisites

- The OLT is connected to the BRAS and the multicast source.
- The VLAN of the LAN switch port connected to the OLT is the same as the upstream VLAN of the OLT.
- The ONT has been added to the OLT. For details, see **9.7.1.3 Adding an ONT to an OLT**.

Copyright © Huawei Technologies Co., Ltd.

- The configuration processes on HGWs of different models or in different appearances are similar. This topic describes how to configure the Internet access service on an HG239 that is connected to an ONT upstream through a LAN.

Data Plan

Item	Data
ONT line profile	Profile name: ftth T-CONT ID: 4 GEM port ID: 13
Traffic profile	ID: 8 802.1p priority: 4 CIR: off (unlimited) Priority-based scheduling policy: local-setting
VLAN Plan	Single VLAN tag: ● SVLAN ID: 1000 ● HGW VLAN: 43 ● MVLAN ID: 1000 ● VLAN type: smart ● VLAN attribute: common VLAN translation policy: ● ONT: translates the upstream VLAN of the HGW to an MVLAN. ● OLT: duplicates multicast packets based on PON ports with MVLAN unchanged.
Multicast service data	Multicast protocol: IGMP proxy Multicast version: IGMPv2 Multicast program: dynamic obtaining mode

Procedure

- Configure the OLT.
  1. Configure a traffic profile.

     Configure traffic profile 8. Set the CIR to off (unlimited), priority to 4, and priority-based scheduling policy to local-setting (that is, queues are scheduled based on the priority specified in the profile).

     NOTE

     Run the **display traffic table ip** command to query the existing traffic profiles in the system. If the existing traffic profiles in the system do not meet the requirements, run the **traffic table ip** command to add a traffic profile.

Copyright © Huawei Technologies Co., Ltd.

```
huawei(config)#traffic table ip index 8 cir off priority 4 priority-
policy
local-setting
```

2. Configure the mapping relationship between a GEM port and a VLAN.

   If the ONT is connected to the HGW through Ethernet port 2, map the service flow of Ethernet port 2 to GEM port 13 in the ONT line profile.

```
huawei(config)#ont-lineprofile gpon profile-name ftth
huawei(config-gpon-lineprofile-1)#gem mapping 13 2 vlan 1000
huawei(config-gpon-lineprofile-1)#commit
huawei(config-gpon-lineprofile-1)#quit
```

3. Configure a VLAN translation policy for the Ethernet port on the ONT.

   If the ONT is connected to the HGW through Ethernet port 2, VLAN 43 of the HGW is translated to VLAN 1000 and the MVLAN of the ONT is translated to VLAN 1000.

```
huawei(config)#ont-srvprofile gpon profile-name ftth
huawei(config-gpon-srvprofile-1)#port vlan eth 2 translation 1000 user-
vlan 43
huawei(config-gpon-srvprofile-1)#multicast-forward tag translation 43
huawei(config-gpon-srvprofile-1)#commit
huawei(config-gpon-srvprofile-1)#quit
```

4. Create a service VLAN and add an upstream port to it.

   Add upstream port 0/19/0 to VLAN 1000.

```
huawei(config)#vlan 1000 smart
huawei(config)#port vlan 1000 0/19 0
```

5. Create service flows.

   Set the service VLAN to 1000, GEM port ID to 13, and user VLAN to 1000, and use traffic profile 8.

```
huawei(config)#service-port 1 vlan 1000 gpon 0/1/0 ont 1 gemport 13 multi-
service
 user-vlan 1000 rx-cttr 8 tx-cttr 8
huawei(config)#service-port 2 vlan 1000 gpon 0/1/0 ont 2 gemport 13 multi-
service
 user-vlan 1000 rx-cttr 8 tx-cttr 8
```

6. Create an MVLAN and configure the IGMP version.

   Set the IGMP version for the MVLAN to IGMPv2.

```
huawei(config)#multicast-vlan 1000
huawei(config-mvlan1000)#igmp version v2
  This operation will delete all IPv4 programs with source IP addresses in
the
current multicast VLAN
  Are you sure to change current IGMP version? (y/n)[n]:y
  Command is being executed. Please wait...
  Command has been executed successfully
```

7. Configure a program library.

   Set the mode for obtaining multicast programs to dynamic.

   NOTE

   You can set the mode for obtaining multicast programs to dynamic only when the IGMP mode is off.

```
huawei(config-mvlan1000)#igmp mode off
  Are you sure to close IGMP? (y/n)[n]:y
  Command is being executed. Please wait...
```


Copyright © Huawei Technologies Co., Ltd.

```
  Command has been executed successfully

huawei(config-mvlan1000)#igmp match mode disable
  Command has been executed successfully
```

(Optional) Set the address range for the dynamic programs. If you need to limit the address range of dynamic programs, perform this operation. For example, set the address range of dynamic programs to 224.1.1.1-224.1.1.100.

```
huawei(config-mvlan1000)#igmp match group ip 224.1.1.1 to-ip 224.1.1.100
```

8. Set the IGMP mode.

   Select the IGMP proxy mode.

   ```
   huawei(config-mvlan1000)#igmp mode proxy
     Are you sure to change IGMP mode? (y/n)[n]:y
     Command is being executed. Please wait...
     Command has been executed successfully
   ```

9. Configure the IGMP upstream port.

   Set the IGMP upstream port ID to 0/19/0 and working mode to **default**. Protocol packets are transmitted to all the IGMP upstream ports in the multicast VLAN.

   ```
   huawei(config-mvlan1000)#igmp uplink-port 0/19/0
   huawei(config-mvlan1000)#btv
   huawei(config-btv)#igmp uplink-port-mode default
   Are you sure to change the uplink port mode?(y/n)[n]:y
   ```

10. (Optional) Set multicast global parameters.

    In this example, the default settings are used for all the multicast global parameters.

11. Configure multicast users.

    Add service ports 1 and 2 as multicast users.

    ```
    huawei(config-btv)#igmp user add service-port 1
    huawei(config-btv)#igmp user add service-port 2
    huawei(config-btv)#multicast-vlan 1000
    huawei(config-mvlan1000)#igmp multicast-vlan member service-port 1
    huawei(config-mvlan1000)#igmp multicast-vlan member service-port 2
    huawei(config-mvlan1000)#quit
    ```

12. Save the data.

    ```
    huawei(config)#save
    ```

- Configure the HGW.

  1. Log in to the Web configuration window.

     a. Enter http://192.168.1.1/cu.html (default IP address) to the address bar of the Internet Explorer (IE) and press Enter.

     b. In the login dialog box, enter the user name and password of the administrator (the Internet service provider (ISP) provides the default user name and default password). Then, click **OK**.

  2. Set parameters for the BTV service.

     This example assumes LAN3 as an BTV port.

     a. Choose **Network** > **Bandwidth Configuration** from the navigation tree.

     b. In the right pane, create LAN connection 3 for the BTV service. Set the parameters as follows:

Copyright © Huawei Technologies Co., Ltd.

Parameter	Value
Bearing service	**OTHER**: The connection is used for the BTV service.
VLAN enabling	**Enable** VLAN tags are added to upstream packets. **NOTE** When BTV service flows are created on the OLT, the value is **Disable** if **uservlan** is untagged and the value is **Enable** if **uservlan** is tagged.
VLANID [1-4094]	VLAN ID corresponding to the user VLAN value for BTV service flows created on the OLT. In this example, set this parameter to 43.
Binding item	LAN3
Mode	Bridge
DHCP transparent transmission	Enable

c. Click **OK** to save the settings.

3. Restart the HGW.

   Choose **Management** > **Device Management** and click **Restarting the Device**.

----End

9.7.2.7 Configuring the VoD Service

The OLT is connected to the remote bridging ONT through a GPON port to provide users with the VoD service.

Prerequisites

- The OLT is connected to the BRAS and the program source.
- The VLAN of the LAN switch port connected to the OLT is the same as the upstream VLAN of the OLT.
- The ONT has been added to the OLT. For details, see **9.7.1.3 Adding an ONT to an OLT**.
- The configuration processes on HGWs of different models or in different appearances are similar. This topic describes how to configure the Internet access service on an HG239 that is connected to an ONT upstream through a LAN.

Copyright © Huawei Technologies Co., Ltd.

Data Plan

Item	Data
ONT line profile	Profile name: ftth T-CONT ID: 4 GEM port ID: 13
Traffic profile	ID: 8 802.1p priority: 4 CIR: off (unlimited) Priority-based scheduling policy: local-setting
VLAN Plan	Single VLAN tag: ● SVLAN ID: 1100 ● VLAN type: smart ● VLAN attribute: common ● UVLAN (upstream VLAN of the HGW): 41 ● CVLAN=UVLAN VLAN translation policy: ● ONT: transparently transmits the UVLAN of the HGW. ● OLT: implements VLAN translation: U<->S.

Procedure

Step 1 Configure the OLT.

1. Configure a traffic profile.

   Configure traffic profile 8. Set the CIR to off (unlimited), priority to 4, and priority-based scheduling policy to local-setting (that is, queues are scheduled based on the priority specified in the profile).

   NOTE

   Run the **display traffic table ip** command to query the existing traffic profiles in the system. If the existing traffic profiles in the system do not meet the requirements, run the **traffic table ip** command to add a traffic profile.

   ```
   huawei(config)#traffic table ip index 8 cir off priority 4 priority-policy
   local-setting
   ```

2. Configure the mapping relationship between a GEM port and a VLAN.

   The service flow of user VLAN 41 is mapped to GEM port 13 in the ONT line profile.

   ```
   huawei(config)#ont-lineprofile gpon profile-name ftth
   huawei(config-gpon-lineprofile-1)#gem mapping 13 4 vlan 41
   huawei(config-gpon-lineprofile-1)#commit
   huawei(config-gpon-lineprofile-1)#quit
   ```

3. Configure the VLAN of the Ethernet port on the ONT.

Copyright © Huawei Technologies Co., Ltd.

If the ONT is connected to the HGW through Ethernet port 2, add Ethernet port 2 to VLAN 41.

```
huawei(config)#ont-srvprofile gpon profile-name ftth
huawei(config-gpon-srvprofile-1)#port vlan eth 2 41
huawei(config-gpon-srvprofile-1)#commit
huawei(config-gpon-srvprofile-1)#quit
```

4. Create a service VLAN and add an upstream port to it.

   Add upstream port 0/19/0 to VLAN 1100.

   ```
   huawei(config)#vlan 1100 smart
   huawei(config)#port vlan 1100 0/19 0
   ```

5. Create service flows.

   Set the service VLAN to 1100, GEM port ID to 13, and user VLAN to 41, and use traffic profile 8.

   ```
   huawei(config)#service-port 3 vlan 1100 gpon 0/1/0 ont 1 gemport 13
   multi-service user-vlan 41 rx-cttr 8 tx-cttr 8
   huawei(config)#service-port 4 vlan 1100 gpon 0/1/0 ont 2 gemport 13
   multi-service user-vlan 41 rx-cttr 8 tx-cttr 8
   ```

6. Save the data.

   ```
   huawei(config)#save
   ```

Step 2 Configure the HGW.

1. Log in to the Web configuration window.

   a. Enter http://192.168.1.1/cu.html (default IP address) to the address bar of the Internet Explorer (IE) and press Enter.

   b. In the login dialog box, enter the user name and password of the administrator (the Internet service provider (ISP) provides the default user name and default password). Then, click **OK**.

2. Set parameters for the VoD service.

   This example assumes LAN4 as an VoD port.

   a. Choose **Network** > **Bandwidth Configuration** from the navigation tree.

   b. In the right pane, create LAN connection 4 for the VoD service. Set the parameters as follows:

Parameter	Value
Bearing service	**OTHER**: The connection is used for the VoD service.
VLAN enabling	**Enable** VLAN tags are added to upstream packets. **NOTE** When VoD service flows are created on the OLT, the value is **Disable** if **uservlan** is untagged and the value is **Enable** if **uservlan** is tagged.
VLANID [1-4094]	VLAN ID corresponding to the user VLAN value for VoD service flows created on the OLT. In this example, set this parameter to 41.
Binding item	LAN4
Mode	Bridge

Copyright © Huawei Technologies Co., Ltd.

Parameter	Value
DHCP transparent transmission	Enable

c. Click **OK** to save the settings.

3. Restart the HGW.

   Choose **Management** > **Device Management** and click **Restarting the Device**.

----End

9.7.2.8 Configuring Link Aggregation, Congestion Control, and Security Policy

The global configuration of link aggregation and queue scheduling based on priorities ensures service reliability. The global configuration of security policies ensures service security.

Context

Link aggregation provides a higher bandwidth and uplink reliability for optical line terminals (OLTs) by aggregating multiple uplink Ethernet ports to one link aggregation group (LAG). Link aggregation is recommended.

Congestion control places the packets to be sent from a port into multiple queues that are marked with different priorities. Then, the packets are sent based on queue priorities. Congestion control is recommended.

Security policies ensure system, user, and service security.

NOTE

Enable a service security function based on the service type. For details, see **9.6.6 Principle of Security Data Plan**.

Procedure

- Configure link aggregation.

  The following configurations are used as an example to configure link aggregation:

  - Uplink ports 0/19/0 and 0/19/1 are added to a LAG.
  - The two ports send packets upstream based on the packets' source MAC addresses.
  - The LAG works in Link Aggregation Control Protocol (LACP) static aggregation mode.

  ```
  huawei(config)#link-aggregation 0/19 0-1 ingress workmode lacp-static
  ```

- Configure queue scheduling.

  According to quality of service (QoS) planning principles, all packets are scheduled in strict priority (SP) mode and mapped to queues according to the packets' priorities. For details about QoS planning principles, see **11.2.2 Principle of QoS Data Plan**.

  ```
  huawei(config)#queue-scheduler strict-priority
  huawei(config)#cos-queue-map cos0 0 cos4 4 cos5 5 cos6 6
  ```

- Configure system security.

  - Enable deny of service (DoS) anti-attack on the OLT.

Copyright © Huawei Technologies Co., Ltd.

1. Run the **security anti-dos enable** command to globally enable DoS anti-attack.
2. Run the **security anti-dos control-packet policy** command to configure a protocol packet processing policy that will be used when a DoS attack occurs.
3. Run the **security anti-dos control-packet rate** command to configure the threshold for the rate of sending protocol packets to the CPU.

- Enable IP address anti-attack on the OLT.

  Run the **security anti-ipattack enable** command to enable IP address anti-attack.

- Configure user security.
  - Enable MAC address anti-flapping on the OLT.

    Run the **security anti-macduplicate enable** command to enable MAC address anti-flapping.
  - Enable MAC address anti-spoofing on the OLT.
    1. In global config mode, run the **security anti-macspoofing enable** command to globally enable MAC address anti-spoofing.
    2. Enable MAC address anti-spoofing at VLAN level in global config mode or service profile mode:
       a. In global config mode, run the **security anti-macspoofing vlan** command to enable MAC address anti-spoofing.
       b. In global config mode, run the **vlan service-profile** command to create a VLAN service profile.
       c. Perform the following operations to enable MAC address anti-spoofing in VLAN service profile mode:
          a. Run the **security anti-macspoofing enable** command to enable MAC address anti-spoofing at VLAN level.
          b. Run the **commit** command to make the profile configuration take effect.
          c. Run the **quit** command to quit the VLAN service profile mode.
          d. Run the **vlan bind service-profile** command to bind the created VLAN service profile to a VLAN.
    3. (Optional) Run the **security anti-macspoofing max-mac-count** command to set the maximum number of MAC addresses that can be bound to a service flow.
    4. (Optional) Run the **security anti-macspoofing exclude** command to configure the types of packets for which MAC address anti-spoofing does not take effect, such as Internet Group Management Protocol (IGMP) packets.
  - Enable IP address anti-spoofing on the OLT.

    IP address anti-spoofing can be enabled or disabled at three levels: global, VLAN, and service port levels. This function takes effect only after it is enabled at the three levels. Among the three levels, IP address anti-spoofing is disabled only at the global level by default.
    1. In global config mode, run the **security anti-ipspoofing enable** command to enable IP address anti-spoofing at the global level.
    2. In VLAN service profile mode, run the **security anti-ipspoofing enable** command to enable IP address anti-spoofing at the VLAN level.

Copyright © Huawei Technologies Co., Ltd.

3. Run the **security anti-ipspoofing service-port** *serviceport-id* **enable** command to enable IP address anti-spoofing at the service port level.

- Configure service security.
  - Enable Dynamic Host Configuration Protocol (DHCP) Option 82 on the OLT. This configuration is recommended for the DHCP-based Internet access service.
    1. Enable DHCP Option 82 on the OLT.

       DHCP Option 82 can be enabled or disabled at four levels: global, port, VLAN, and service port levels. This function takes effect only after it is enabled at the four levels. Among the four levels, DHCP Option 82 is disabled only at the global level by default.

       - The global level: In global config mode, run the **dhcp option82** command to enable DHCP Option 82 at the global level.

         When you run this command, select the **enable**, **forward**, or **rebuild** parameter based on site requirements. The three parameters can all enable DHCP Option 82 but provide different packet processing policies on the OLT. For details, see the **dhcp option82** command.
       - The port level: In global config mode, run the **dhcp option82 port** or **dhcp option82 board** command to enable DHCP Option 82 at the port level.
       - The VLAN level:
         a. In global config mode, run the **vlan service-profile** command to create a VLAN service profile.
         b. Run the **dhcp option82 enable** command to enable DHCP Option 82 at the VLAN level.
         c. Run the **commit** command to make the profile configuration take effect.
         d. Run the **quit** command to quit the VLAN service profile mode.
         e. Run the **vlan bind service-profile** command to bind the created VLAN service profile to a VLAN.
       - The service port level: In global config mode, run the **dhcp option82 service-port** command to enable DHCP Option 82 at the service port level.
    2. On the OLT, run the **dhcp-option82 permit-forwarding service-port** command with the **enable** parameter selected, to allow ONT DHCP packets to carry Option 82 information.
  - Enable Policy Information Transfer Protocol (PITP) on the OLT. This configuration is recommended for the PPPoE-based Internet access service.
    1. Enable PITP on the OLT.

       PITP can be enabled or disabled at four levels: global, port, VLAN, and service port levels. This function takes effect only after it is enabled at the four levels. Among the four levels, PITP is disabled only at the global level by default.

       - The global level: In global config mode, run the **pitp enable pmode**, **pitp forward pmode**, or **pitp rebuild pmode** command to enable PITP at the global level.

         In the preceding commands, the **enable**, **forward**, and **rebuild** parameters can all enable PITP but provide different packet processing policies on the

Copyright © Huawei Technologies Co., Ltd.

OLT. Select one of them based on site requirements. For details, see the **pitp** command.

- The port level: In global config mode, run the **pitp port** or **pitp board** command to enable PITP at the port level.
- The VLAN level:
  a. In global config mode, run the **vlan service-profile** command to create a VLAN service profile.
  b. Run the **pitp enable** command to enable PITP at the VLAN level.
  c. Run the **commit** command to make the profile configuration take effect.
  d. Run the **quit** command to quit the VLAN service profile mode.
  e. Run the **vlan bind service-profile** command to bind the created VLAN service profile to a VLAN.
- The service port level: In global config mode, run the **pitp service-port** command to enable PITP at the service port level.

2. On the OLT, run the **pitp permit-forwarding service-port** command with the **enable** parameter selected, to allow ONT PPPoE packets to carry a vendor tag.

----End

9.7.2.9 Verifying Services

In the FTTH scenario, ONTs are installed in users' houses which are far away from the central equipment room. ONTs provide remote service verification methods including PPPoE dialup emulation, call emulation, and multicast emulation to facilitate configuration and commissioning engineers to verify services remotely after service configuration.

Prerequisites

ONTs and upper-layer devices have been connected properly. The BRAS and MGC/IMS have been configured.

Background

Remote Service Verification Method	Function	Description
PPPoE dialup emulation	An ONT simulates a PPPoE user terminal software to perform dialup and interact with the BRAS to verify the connectivity between the ONT and BRAS.	● PPPoE dialup emulation requires a service flow which does not belong to a QinQ VLAN. ● A user name, password, and authentication mode must be configured on the BRAS for the PPPoE dialup emulation. ● An ONT supports a maximum of a PPPoE dialup emulation.

Copyright © Huawei Technologies Co., Ltd.

Remote Service Verification Method	Function	Description
Call Emulation	An ONT simulates a voice user to make a call to check whether the voice service data is correctly configured. You can also use the call emulation function to locate a fault when the voice service is faulty.	● An ONT can simulate a caller or callee to communicate with a phone in a call. In this case, only a functional phone is required in the central office where the acceptance personnel is. ● An ONT supports a maximum of a call emulation.
Multicast emulation	This function enables you to simulate a multicast user going online and lead the program stream to an ONT. You can check whether the multicast service is normal by checking the real-time traffic of the multicast program.	Multicast services configured in the dynamic controllable multicast mode do not support this function.

Data plan

Item	Data	Remarks
PPPoE dialup emulation parameters	PPPoE user name: test@huawei Password: test	The user name, password, and authentication mode for the emulation test must be configured on the BRAS. The entered user name, password, and authentication mode must be consistent with those configured on the BRAS.
Call emulation parameters	ONT POTS ID: 1	The default values are used. You can run the **display pots emulational configuration** command to check the parameter values.
Multicast emulation parameters	Multicast service flow ID: 1 MVLAN: 1000 IP address of the multicast program: 224.1.1.10	-

Procedure

- Verify the Internet access service using PPPoE dialup emulation.
  1. In the xPON board mode, run the **pppoe simulate start** command to start a PPPoE dialup emulation test. The following test uses GPON as an example:

Copyright © Huawei Technologies Co., Ltd.

```
huawei(config)#interface gpon 0/1
huawei(config-if-gpon-0/1)#pppoe simulate start
{ portid<U><0,7> }:0
{ ontid<U><0,127> }:1
{ eth<K>|untagged<K>|vlanid<U><0,4095> }:eth
{ ont-portid<U><1,8> }:4
{ untagged<K>|vlanid<U><0,4095> }:100
{ priority<U><0,7>|user-name<K> }:user-name
{ username<S><Length 1-64> }:test@huawei
{ user-password<K> }:user-password
{ password<S><Length 1-64> }:test
{ authentication-mode<K> }:authentication-mode
{ protocol<E><chap,pap> }:chap

  Command:
          pppoe simulate start 0 1 eth 4 100 user-name test@huawei user-
password
 test authentication-mode chap

huawei(config-if-gpon-0/1)#
  ---------------------------------
  ONT PPPoE Test Result
  ---------------------------------
  F/S/P                : 0/1/0
  ONT-ID               : 1
  ONT ETH Port ID      : 4
  ONT Vlan ID          : 100
  Vlan Priority        : -
  Emluator result      : Success
  Session ID           : 18814
  User IP              : 192.168.100.101
  Gateway IP           : 192.168.100.1
  ---------------------------------
```

- Troubleshooting methods for the Internet access service
  1. Check whether configurations are complete on the OLT.
     - Run the **display ont info** command to query the ONT status to check whether the ONT is registered successfully.
     - Run the **display service-port** command to check whether the Internet access service flow is configured and whether the inner VLAN ID of the service flow is consistent with that in the data plan.
     - If a native VLAN is configured for the Ethernet port on the ONT, run the **display ont port attribute** command in the xPON board mode to check whether the native VLAN is correct.
  2. Check the upstream and downstream ports by checking the MAC address learning status.
     a. Run the **display mac-address vlan** command to check the MAC address learning status of the Internet service VLAN.
        - If the upstream port does not learn a MAC address, check the network connections between the upstream port and upper-layer devices and check the configurations of upper-layer devices.
        - If the downstream port does not learn a MAC address, check whether the ONT is activated, whether the PC is connected to the right port on the ONT, and whether the PC is working properly.
     b. Run the **display ont-learned-mac** command to check whether the ONT connecting to the PON port learned any MAC addresses.

Copyright © Huawei Technologies Co., Ltd.

If not, check whether the ONT properly connects to the PC or home gateway (HGW).

- Verify the voice service using call emulation.
  1. Run the **ont emulational call** command to configure a call emulation test.

```
huawei(config)#test
huawei(config-test)#ont emulational call caller-port 0/1/0 1 1 telno
77730020
{ <cr>|caller-stop-time<K> }:

  Command:
          ont emulational call caller-port 0/1/0 1 1 telno 77730020
```

  2. The ONT outputs the call emulation result after the test is complete.

```
huawei(config-test)#
  ------------------------------------------------------------------
  F/S/P                : 0/1/0
  ONT-ID               : 0
  ONT-POTSID           : 1
  Test type            : caller emulational call test
  Detected number      : 77730020
  Reported number      : 77730020
  Current status       : test end
  Test Result          : success
  ------------------------------------------------------------------
```

- Troubleshooting methods for the voice service.
  1. Check whether configurations are complete on the OLT.
     - Run the **display ont info** command to query the ONT status to check whether the ONT is registered successfully.
     - Run the **display service-port** command to check whether the voice service flow is configured and whether the inner VLAN ID of the service flow is consistent with that in the data plan.
  2. Check the upstream and downstream ports by checking the MAC address learning status.

     Run the **display mac-address vlan** command to check the MAC address learning status of the voice service VLAN.
     - If the upstream port does not learn a MAC address, check the network connections between the upstream port and upper-layer devices and check the configurations of upper-layer devices.
     - If the downstream port does not learn a MAC address, check whether the ONT is activated and whether physical links are normal.
     - If both the upstream and downstream ports can learn the MAC address, record the MAC address of the ONT and log in to the service router (SR) to check whether an IP address is allocated to the MAC address.
  3. Check the registration status of the voice service.
     - You can run the **display ont port state** command on the OLT to query the call connection status on the POTS port. If **Call State** is **RegisterFail** or **Connecting** for a long time, check whether the voice configuration on the MGC/SIP server is consistent with that on the ONT.
     - If the ONT uses the H.248 protocol, you can run the **display ont mg status** command on the OLT to query the registration status of the MG interface that connects to the ONT. If **MG Status** is **UnRegistered** or **Registering** for a long

Copyright © Huawei Technologies Co., Ltd.

time, check whether the voice configuration on the MGC/SIP server is consistent with that on the ONT.

- You can query the registration status of the voice service on the ONT web page. If the query result shows that the registration fails or the voice service is in the registering state for a long time, check whether the voice configuration on the MGC/SIP server is consistent with that on the ONT.

- Verify the multicast service using multicast emulation.

  1. Run the **igmp static-join** command to simulate a multicast user to order a multicast program.

     ```
     huawei(config)#btv
     huawei(config-btv)#igmp static-join service-port 1 ip 224.1.1.10 vlan 1000
     ```

     NOTE

     If the multicast program is obtained dynamically, **igmp static-join** can be executed successfully only when the range for obtaining the dynamic program is set.

  2. Run the **display igmp user** command to query the status of the multicast user.

     ```
     huawei(config-btv)#display igmp user service-port 1
       User                        : 0/1/0/1
       State                       : online
       Authentication              : no-auth
       Quick leave                 : MAC-based
       IGMP flow ID                : 1
       Video flow ID               : 1
       Log switch                  : enable
       Bind profiles               : -
       IGMP version                : IGMP v3
       Current version             : IGMP v3
       Current IGMP IPv6 version   : IGMP IPv6 v2
       Available programs          : 8
       Global leave                : disable
       User max bandwidth          : no-limit
       Used bandwidth(kbps)        : 0
       Used bandwidth
       to max bandwidth(%)         : -
       Total video bandwidth       : -
       Mcast video bandwidth       : -
       Active program list

     ------------------------------------------------------------------------
     --
       Program name     VLAN  IP/MAC           State           Start time

     ------------------------------------------------------------------------
     --
       PROGRAM-5        1000  224.1.1.10       watching        2011-10-29
                                                               16:33:41+08:00

     ------------------------------------------------------------------------
     --
       Total: 1
     ```

  3. Run the **display multicast flow-statistic** command to query the real-time traffic of the multicast program.

     ```
     huawei(config-btv)#display multicast flow-statistic vlan 1000 ip
     224.1.1.10
     { <cr>|sourceip<K> }:

       Command:
               display multicast flow-statistic vlan 1000 ip 224.1.1.10
     ```


Copyright © Huawei Technologies Co., Ltd.

```
Command is being executed. Please wait...
Multicast flow statistic result: 8736(kbps)
```

----End

9.7.3 Gateway ONT Network Scenario

This topic describes how to configure Internet access service, voice service, BTV service and VoD service when gateway ONT are used to build an FTTH network.

9.7.3.1 Service Requirements and Application Scenario

Service Requirements

Optical fibers are connected to users' home and triple play services are required. The following provides detailed service requirements:

- Internet access of multiple PCs in a home is supported.
- Access of multiple telephones in a home is supported.
- IPTV programs can be previewed and watched using STBs.
- Service expansibility is supported and different services do not affect each other.
- Service security is ensured.
  - Internet access services are protected against unauthorized access, user account theft or borrowing, MAC/IP spoofing, and malicious attack.
  - Voice and IPTV services are protected against MAC/IP spoofing, malicious attack, and traffic flooding attack.
- Service faults are easy to locate and services are easy to maintain.

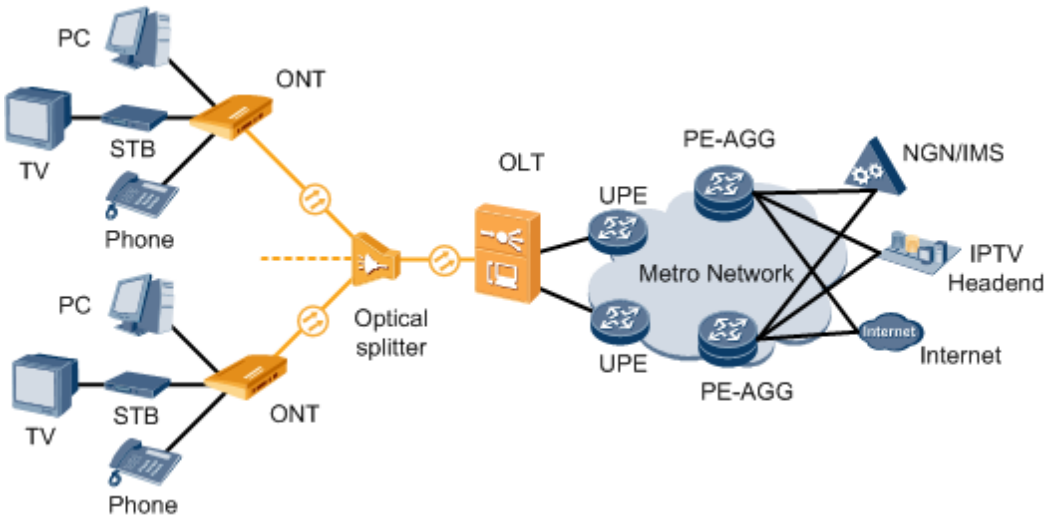
Application Scenario

As shown in **Figure 9-5**, the ONT integrating an IAD provides Internet, VoIP, and IPTV services to users.

The HGW ONT facilitates interconnection of home devices by providing Layer 3 services, such as Point-to-Point Protocol over Ethernet (PPPoE)/DHCP dial-up, network address translation (NAT), and Internet Group Management Protocol (IGMP) snooping. This scenario provides fine-grained management channels and service control, and mainly applies to Layer 3 networking.

Copyright © Huawei Technologies Co., Ltd.

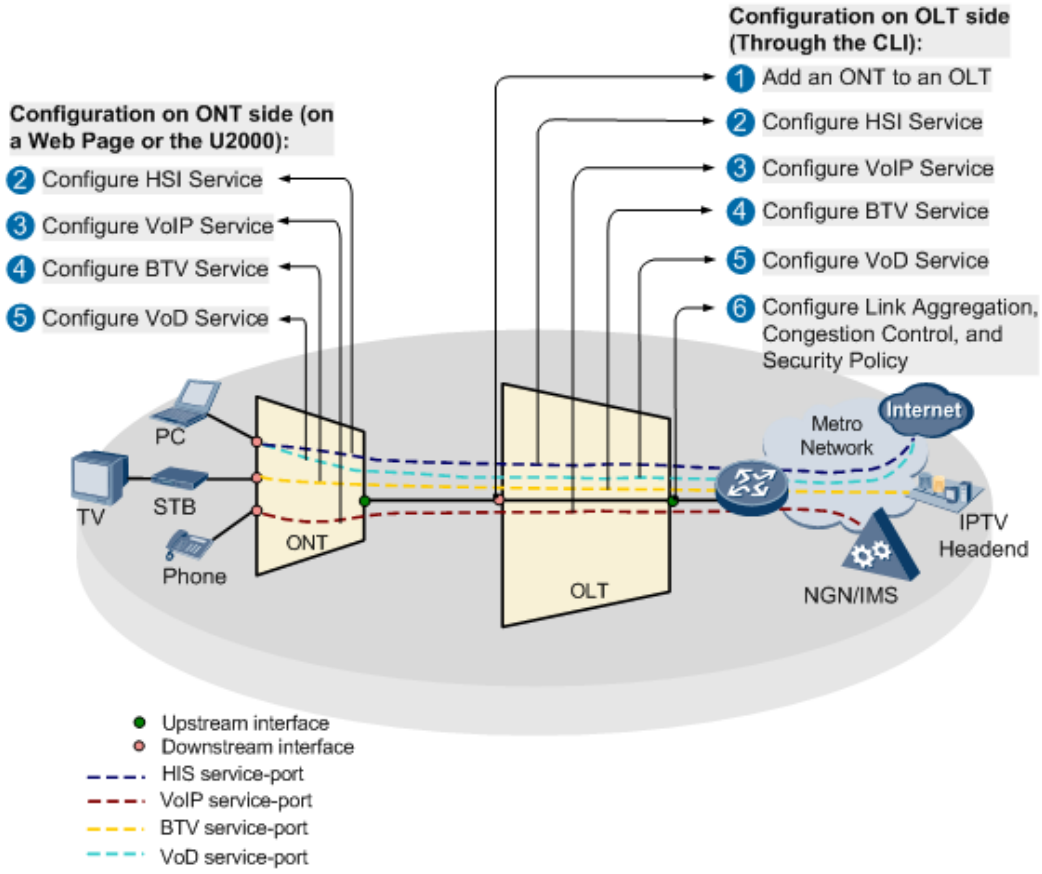
Figure 9-5 HGW ONT



9.7.3.2 Configuration Process

Figure 9-6 shows the configuration roadmap in fiber to the home (FTTH) networking using a gateway optical network terminal (ONT).

Figure 9-6 Configuration roadmap in FTTH networking using a gateway ONT



Copyright © Huawei Technologies Co., Ltd.

The following table describes the configuration steps.

Item	Step		Description
Optical line terminal (OLT)	**9.7.1.3 Adding an ONT to an OLT**		Services can be configured for an ONT only after the ONT is successfully added to an OLT.
OLT ONT U2000	**9.7.3.4 Configuring the Internet Access Service (on a Web Page or the U2000)**		None

	Configure the VoIP service.	**9.7.3.5 Configuring the H.248-based Voice Service (on a Web Page or the U2000)**	**NOTE**
			● The H.248 and Session Initiation Protocol (SIP) protocols are mutually exclusive for the VoIP service. Either of them is configured at a time.
			● The voice service can be configured through command line interface (CLI) on an OLT, web page, or U2000. Select a configuration mode based on site requirements.
			  ● OLT CLI: This mode can be used for site deployment or the U2000 has not been deployed.
			  ● Web page: This mode can be used to configure voice parameters after the service channel has been configured through the OLT CLI. It can be used for site deployment.
			  ● U2000: This mode can be used to configure voice parameters after the service channel has been configured through the OLT CLI. It can be used for service provisioning in batches.

		9.7.3.6 Configuring the H.248-based Voice Service (Through the CLI)	
		9.7.3.7 Configuring the SIP-based Voice Service (on a Web Page or the U2000)	
		9.7.3.8 Configuring the SIP-based Voice Service (Through the CLI)	
	Configure the IPTV service.	**9.7.3.9 Configuring the BTV Service**	IPTV services include the BTV and VoD services that are different in configuration procedures and need to be configured separately.
		9.7.3.10 Configuring the VoD Service	

Copyright © Huawei Technologies Co., Ltd.

Item	Step	Description
OLT	9.7.1.11 Configuring Link Aggregation, Congestion Control, and Security Policies	The global configuration of link aggregation and queue scheduling based on priorities ensures service reliability. The global configuration of security policies ensures service security.
OLT	9.7.1.12 Verifying Services	The OLT provides remote verification methods including ONT PPPoE/DHCP dialup emulation and call emulation for configuration and commissioning engineers to verify services remotely after service configuration, avoiding a second on-site operation.

9.7.3.3 Adding an ONT to an OLT

Services can be configured for an ONT only after the ONT is successfully added to an OLT.

Data Plan

Table 9-5 Data plan

Item	Data
DBA profile	Profile name: ftth_dba Profile type: type3 Assured bandwidth: 8 Mbit/s Maximum bandwidth: 20 Mbit/s
ONT line profile	Profile name: ftth T-CONT ID: 4 GEM port ID for management services: 11 GEM port ID for voice services: 12 GEM port ID for video services: 13 GEM port ID for Internet access services: 14
ONT service profile	Profile name: ftth ONT port capability set: adaptive
Network topology data	PON port: 0/1/0 ONT IDs: 1 and 2

Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Configure GPON ONT profiles.

GPON ONT profiles include the DBA profile, line profile, service profile, and alarm profile.

- DBA profile: A DBA profile describes GPON traffic parameters. A T-CONT is bound to a DBA profile for dynamic bandwidth allocation, improving upstream bandwidth utilization.
- Line profile: A line profile describes the binding between the T-CONT and the DBA profile, the QoS mode of the traffic stream, and the mapping between the GEM port and the ONT-side service.
- Service profile: A service profile provides the service configuration channel for the ONT that is managed by using optical network terminal management and control interface (OMCI).
- Alarm profile: An alarm profile contains a series of alarm thresholds to measure and monitor the performance of activated ONT lines. When a statistical value reaches the threshold, the host is notified and an alarm is reported to the log host and the NMS.

1. Configure a DBA profile.

   Run the **display dba-profile** command to query existing DBA profiles in the system. If the existing DBA profiles in the system do not meet the requirements, run the **dba-profile add** command to add a DBA profile.

   Create the same DBA profile for different types of services. Set the profile name to **ftth_dba**, profile type to **type3**, assured bandwidth to 8 Mbit/s, and maximum bandwidth to 20 Mbit/s.

   ```
   huawei(config)#dba-profile add profile-name ftth_dba type3 assure 8192 max
   20480
   ```

   NOTE

   The DBA implementation is based on an ONT. Therefore, select a DBA profile of the proper bandwidth type and configure proper bandwidth according to the service types and total user count of the ONT. Note that the sum of the fixed bandwidth and the assured bandwidth must not be greater than the total bandwidth of the PON port.

2. Configure an ONT line profile.

   Create a GPON ONT line profile, named **ftth**, and bind it to the DBA profile **ftth_dba**.

   ```
   huawei(config)#ont-lineprofile gpon profile-name ftth
   huawei(config-gpon-lineprofile-1)#tcont 4 dba-profile-name ftth_dba
   ```

   Create different GEM ports according to different service types, in which

   - GEM port 11 is used to carry management services.
   - GEM port 12 is used to carry voice services.
   - GEM port 13 is used to carry video services.
   - GEM port 14 is used to carry Internet access services.

   ```
   huawei(config-gpon-lineprofile-1)#gem add 11 eth tcont 4
   huawei(config-gpon-lineprofile-1)#gem add 12 eth tcont 4
   huawei(config-gpon-lineprofile-1)#gem add 13 eth tcont 4
   huawei(config-gpon-lineprofile-1)#gem add 14 eth tcont 4
   ```

   NOTE

   1. To change the default QoS mode, run the **qos-mode** command to set the QoS mode to **gem-car** or **flow-car**, and run the **gem add** command to set the index of the traffic profile bound to the GEM port.
   2. When the QoS mode is priority-queue (PQ), the default queue priority is 0; when the QoS mode is flow-car or gem-car, traffic profile 6 is bound to the GEM port by default (no rate limitation).

Copyright © Huawei Technologies Co., Ltd.

After the configurations are complete, run the **commit** command to apply the parameters settings.

```
huawei(config-gpon-lineprofile-1)#commit
huawei(config-gpon-lineprofile-1)#quit
```

3. Configure an ONT service profile.

   Create a GPON ONT service profile, named **ftth**. Configure the capability set of the ETH port and POTS port to **adaptive**. Then the system automatically adapts to the ONT according to the actual capability of the online ONT.

   ```
   huawei(config)#ont-srvprofile gpon profile-name ftth
   huawei(config-gpon-srvprofile-1)#ont-port eth adaptive pots adaptive
   ```

   After the configurations are complete, run the **commit** command to apply the parameters setting.

   ```
   huawei(config-gpon-srvprofile-1)#commit
   huawei(config-gpon-srvprofile-1)#quit
   ```

4. (Optional) Add an alarm profile.
   - The default GPON alarm profile 1 is used. The alarm thresholds of the default alarm profile are 0, which indicates that no alarm is generated.
   - In this example, the default alarm profile is used, and therefore the configuration of the alarm profile is not required.
   - Run the **gpon alarm-profile add** command to configure a GPON alarm profile, which is used for monitoring the performance of an activated ONT line.

Step 2 Add an ONT.

Connect two ONTs to GPON port 0/1/0. Set the ONT IDs to **1** and **2**, SNs to **32303131D659FD40** and **6877687714852901**, passwords to **0100000001** and **0100000002**, discovery mode for password authentication to **once-on**, and management mode to **OMCI**. Bind the two ONTs to ONT line profile **ftth** and ONT service profile **ftth**.

There are two methods of adding an ONT: add an ONT offline and confirm an automatically discovered ONT.

- Add ONTs offline.

  If the password of an ONT is known, run the **ont add** command to add an ONT offline.

  ```
  huawei(config)#interface gpon 0/1
  huawei(config-if-gpon-0/1)#ont add 0 1 password-auth 0100000001 once-on no-aging
  omci ont-lineprofile-name
   ftth ont-srvprofile-name ftth
  huawei(config-if-gpon-0/1)#ont add 0 2 password-auth 0100000002 once-on no-aging
  omci ont-lineprofile-name
   ftth ont-srvprofile-name ftth
  ```

- Confirm automatically discovered ONTs.

  If the password or SN of an ONT is unknown, run the **port** ***portid*** **ont-auto-find** command in GPON mode to enable the ONT auto-discovery function of the GPON port. Then, run the **ont confirm** command to confirm the ONT.

  ```
  huawei(config)#interface gpon 0/1
  huawei(config-if-gpon-0/1)#port 0 ont-auto-find enable
  huawei(config-if-gpon-0/1)#display ont autofind 0
    //After this command is executed, the information about all ONTs connected to
  the GPON port through optical splitters is displayed.

  huawei(config-if-gpon-0/1)#ont confirm 0 ontid 1 sn-auth 32303131D659FD40 omci
  ont-lineprofile-name
   ftth ont-srvprofile-name ftth
  ```


Copyright © Huawei Technologies Co., Ltd.

```
huawei(config-if-gpon-0/1)#ont confirm 0 ontid 2 sn-auth 6877687714852901 omci
ont-lineprofile-name
 ftth ont-srvprofile-name ftth
```

NOTE

If multiple ONTs of the same type bound to the same line profile or service profile are connected to the same port, you can bulk add ONTs by bulk confirming automatically discovered ONTs to make configuration easier and more efficient. To do so, the preceding command can be modified as follows:

```
huawei(config-if-gpon-0/1)#ont confirm 0 all sn-auth omci ont-lineprofile-name
ftth
ont-srvprofile-name ftth
```

- (Optional) Bind the alarm profile to the ONT.

  The default profile 1 is used in this example.

```
huawei(config-if-gpon-0/1)#ont alarm-profile 0 1 profile-id 1
huawei(config-if-gpon-0/1)#ont alarm-profile 0 2 profile-id 1
```

Step 3 Check ONT status.

After an ONT is added, run the **display ont info** command to query the current status of the ONT. Ensure that **Config flag** of the ONT is **active**, **Run State** is **online**, **Config state** is **normal**, and **Match state** is **match**.

```
huawei(config-if-gpon-0/1)#display ont info 0 1
  ------------------------------------------------------------------------
  F/S/P                : 0/1/0
  ONT-ID               : 1
  Control flag         : active    //Indicates that the ONT is
activated.
  Run state            : online    //Indicates that the ONT goes online
successfully.
  Config state         : normal    //Indicates that the configuration state of the
ONT is normal.
  Match state          : match     //Indicates that the capability profile bound to
the ONT is consistent with the actual capability of the ONT.
...//The rest of the response information is omitted.
```

When **Config state** is **failed**, **Run state** is **offline**, or **Match state** is **mismatch**:

- If **Control flag** is **deactive**, run the **ont active** command in GPON mode to activate the ONU.
- If **Run state** is **offline**, a physical line may be broken or the optical module may be damaged. Check the line and the optical module.
- If **Config state** is **failed**, the configured ONU capability exceeds the actual ONU capability. In this case, run the **display ont failed-configuration** command in the diagnose mode to check the failed configuration item and the failure cause. Then, rectify the fault accordingly.
- If the ONU does not match, that is, **Match state** is **mismatch**, the port types and number of ports undermatch the actual port types and number of ports supported by the ONU. In this case, run the **display ont capability** command to query the actual capability of the ONU, and then select one of the following modes to modify the ONU configuration:
  - Create a proper ONU profile according to the actual capability of the ONU, and then run the **ont modify** command to modify the configuration data of the ONU.
  - Modify the ONU profile according to the actual capability of the ONU and save the modification. Then, the ONU automatically recovers the configuration successfully.

----End

Copyright © Huawei Technologies Co., Ltd.

9.7.3.4 Configuring the Internet Access Service (on a Web Page or the U2000)

The OLT is connected to the remote ONT through a GPON port to provide users with high-speed Internet access services.

Prerequisites

- The OLT is connected to the BRAS.
- Related configurations are performed on the BRAS according to the authentication and accounting requirements for dialup users. For details about the configurations, see the configuration guide.
- The ONT has been added to the OLT. For details, see **9.7.1.3 Adding an ONT to an OLT**.
- The VLAN of the LAN switch port connected to the OLT is the same as the upstream VLAN of the OLT.

Data Plan

Item	Data
ONT line profile	Profile name: ftth T-CONT ID: 4 GEM port ID: 14
VLAN Plan	Double-tagged VLAN: ● S-VLAN ID: 100 ● S-VLAN type: smart ● S-VLAN attribute: stacking ● CVLAN ID: 1001 ● C'-VLAN ID: 1010-1011 VLAN translation policy: ● ONT: ONTs configure the VLAN and add the same C-VLAN tag to packets. All ONTs are in the same C-VLAN. ● OLT: The OLT performs VLAN translation: C<->S+C'. The C'-VLAN of every ONT differs from each other.

Procedure

- Configure the OLT.
  1. Configure a traffic profile.

     Run the **display traffic table ip** command to query existing traffic profiles in the system. If the traffic profiles existing in the system do not meet the requirements, you need to run the **traffic table ip** command to add a traffic profile.

Copyright © Huawei Technologies Co., Ltd.

Set the profile ID to ftth_hsi, the CIR to 4 Mbit/s, and the priority to 0. In addition, configure the scheduling mode so that packets are scheduled according to their priorities.

```
huawei(config)#traffic table ip name ftth_hsi cir 4096 priority 0 priority-policy local-setting
```

2. Configure the mapping relationship between a GEM port and a VLAN.

   The service flow of user VLAN 1001 is mapped to GEM port 14 in the ONT line profile.

```
huawei(config)#ont-lineprofile gpon profile-name ftth
huawei(config-gpon-lineprofile-1)#gem mapping 14 0 vlan 1001
huawei(config-gpon-lineprofile-1)#commit
huawei(config-gpon-lineprofile-1)#quit
```

3. Create a service VLAN and add an upstream port to it.

   Add upstream port 0/19/0 to VLAN 100.

```
huawei(config)#vlan 100 smart
huawei(config)#vlan attrib 100 stacking
huawei(config)#port vlan 100 0/19 0
```

4. Create service flows.

   Set the service VLAN to 100, GEM port ID to 14, and user VLAN to 1001, and use traffic profile ftth_hsi.

```
huawei(config)#service-port vlan 100 gpon 0/1/0 ont 1 gemport 14 multi-service
user-vlan 1001 tag-transform translate-and-add inner-vlan 1010 inbound traffic-table name
ftth_hsi outbound traffic-table name ftth_hsi
huawei(config)#service-port vlan 100 gpon 0/1/0 ont 2 gemport 14 multi-service
user-vlan 1001 tag-transform translate-and-add inner-vlan 1011 inbound traffic-table name
ftth_hsi outbound traffic-table name ftth_hsi
```

5. Save the data.

```
huawei(config)#save
```

- Configure the ONT on the Web page.

  Log in to the Web page and then configure the ONT on the Web page.

  1. Configure the IP address of the PC network adapter to be in the same network segment with the IP address of the local maintenance Ethernet port on the ONT (default: 192.168.100.1).
  2. Open the Web browser, and enter the IP address (https://192.168.100.1:80 or http://192.168.100.1) (https with high priority is recommended) of the local maintenance Ethernet port on the ONT. In the login window that is displayed, enter the user name (default telecomadmin) and password (default admintelecom) of the administrator. After the password is authenticated, the web configuration window is displayed.

  NOTE

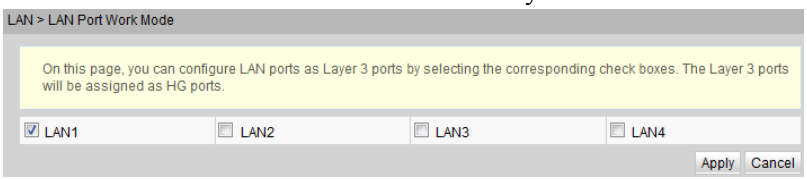
  The Web page for configuring ONT varies with ONT versions, but the parameter configuration is the same. For details, see relevant ONT manuals.

  1. Configure the working mode of a LAN port.

     The LAN port bound to the WAN port must work in the Layer 3 mode. Therefore, set the working mode to Layer 3 for the LAN port connected to the PC.

Copyright © Huawei Technologies Co., Ltd.

a. In the navigation tree, choose **LAN** > **LAN Port Work Mode**. Select the check box of LAN 1 and set LAN1 to work in the Layer 3 mode.



b. Click **Apply**.

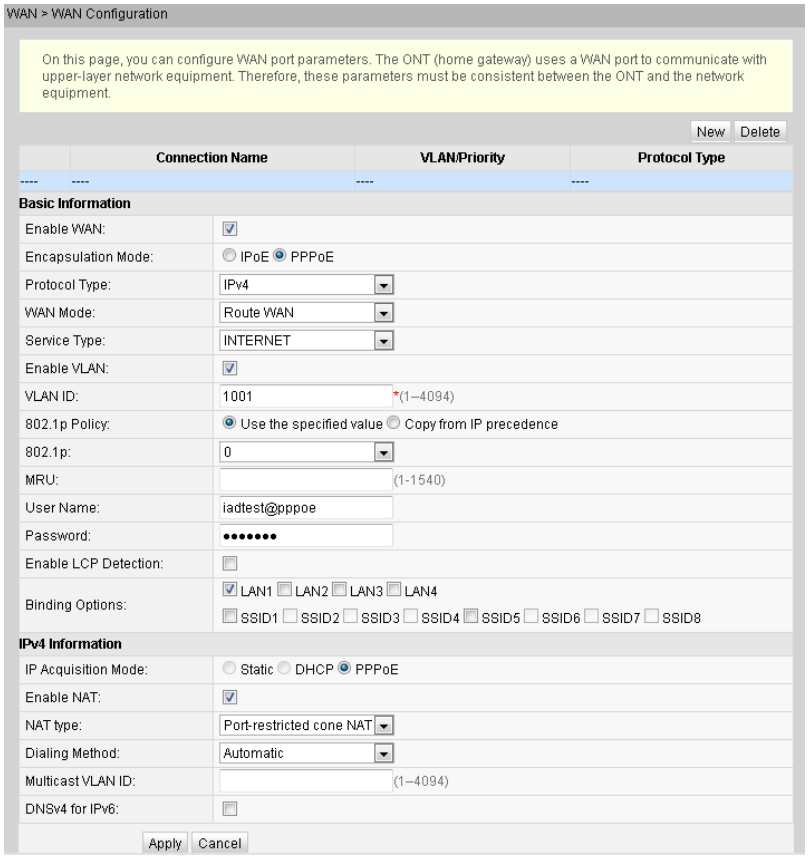
2. Configure parameters of a WAN port.

a. In the navigation tree, choose **WAN** > **WAN Configuration**.

b. In the right pane, click **New**. In the dialog box that is displayed, configure parameters of a WAN port as follows:

- Select **Enable WAN Connection** to enable the new WAN connection.
- Set **Encapsulation mode** to **PPPoE**.
- Set **Mode** to **Route WAN**.
- Set **Service List** to **INTERNET**. (For configuring the Internet access service, **INTERNET** or a combination containing **INTERNET** needs to be selected.)
- Select **Enable VLAN**.
- Set **VLAN ID** to **1001**. (The VLAN ID of the ONT must be the same as the user-side VLAN ID configured on the OLT.)
- Set **802.1p** to **0**.
- Set **User Name** to **iadtest@pppoe** and **Password** to **iadtest**. (The user name and password must be the same as the user name and password configured on the BRAS.)
- Select the check box next to **LAN1** in the **Binding options** area, indicating that the WAN port is bound to LAN1.
- Set **IP Acquisition Mode** to **PPPoE**.
- Select **Enable NAT** to enable the NAT function. (NAT must be enabled to configure the Internet access service.)

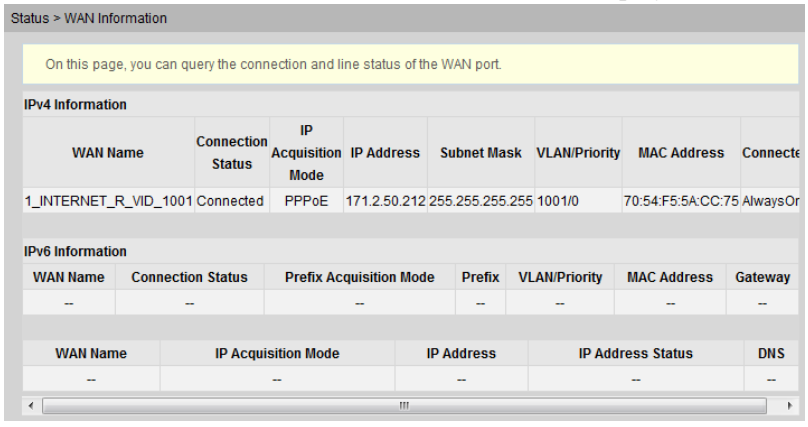
Copyright © Huawei Technologies Co., Ltd.



c. Click **Apply**.

3. Check the ONT connection status.

   In the navigation tree, choose **Status** > **WAN Information**. In the right pane, **Status** is **Connected** and the obtained IP address is displayed at **IP Address**.



- Configure the ONT on the U2000.

  NOTE

  The window for configuring ONT value-added service (VAS) profiles varies with ONT versions, but the parameter configuration is the same. For details, see relevant ONT manuals.

  1. **Add a general VAS configuration profile for the ONT.**

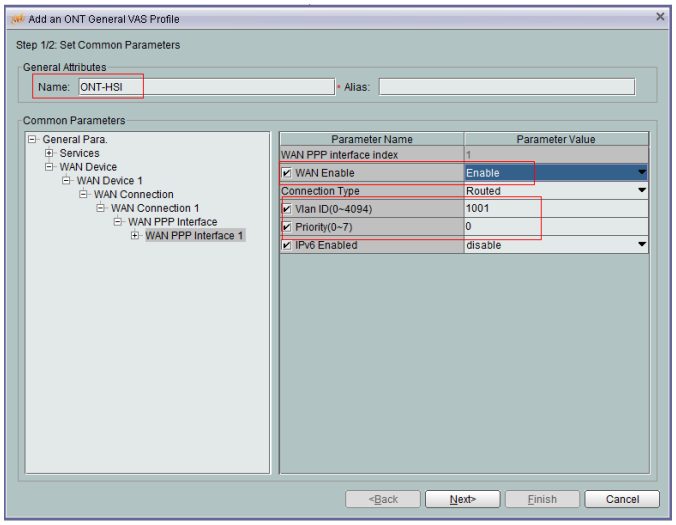
     a. From the main menu, choose **Configuration** > **Access Profile Management**. In the navigation tree of the tab page that is displayed, choose **PON Profile** > **ONT VAS Profile**.

Copyright © Huawei Technologies Co., Ltd.

b. On the **General ONT VAS Profile** tab page, right-click, and choose **Add** from the shortcut menu.

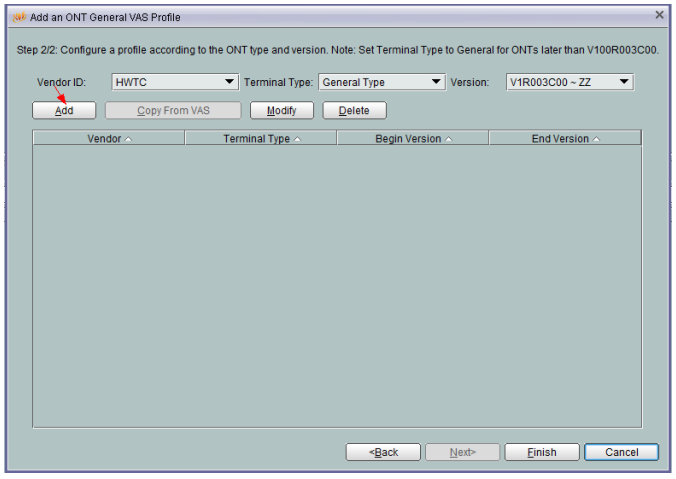
c. Choose **General Para** > **WAN Device** > **WAN Device 1** > **WAN Connection** from the navigation tree, right-click, and choose **Add PPP Connection** from the shortcut menu. Choose the new **WAN PPP Interface 1** and set parameters as follows:

- WAN Enable: Enable
- Connection Type: Routed
- VLAN ID: 1001 (which should be the same as that configured on the OLT at the user side)
- Priority: 0



d. Click **Next**.

e. In the dialog box that is displayed, set **vendor ID** to **HWTC**, **Terminal Type** to **General Type**, and **Version** to **V1R003C00-ZZ**, click **Add**.



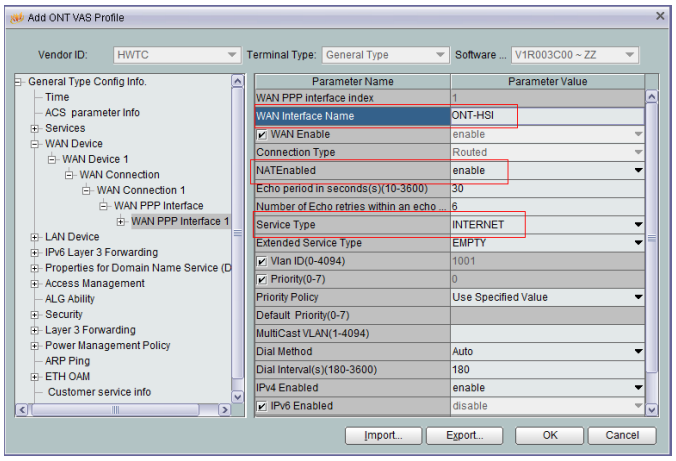
f. Configure a WAN port.

Choose **General Type Config Info** > **WAN Device** > **WAN Device 1** > **WAN Connection** > **WAN Connection 1** > **WAN PPP Interface** > **WAN PPP Interface 1** and set parameters as follows:

- WAN Interface Name: ONT-HSI

Copyright © Huawei Technologies Co., Ltd.

- NATEnabled: enable (Enable the NAT function when configuring the online service.)
- Service Type: INTERNET (For configuring the Internet access service, INTERNET or a combination containing INTERNET needs to be selected.)



g. Configure binding between the WAN port and LAN port.

a. Configure the LAN1 port as a Layer 3 interface.

Choose **General Type Config Info** > **LAN Device** > **LAN Interface 1** > **LAN Interface** > **LAN Ethernet Configuration 1** from the navigation tree. In the right pane, set **LAN port two three-port enable** to **enable**.

NOTE

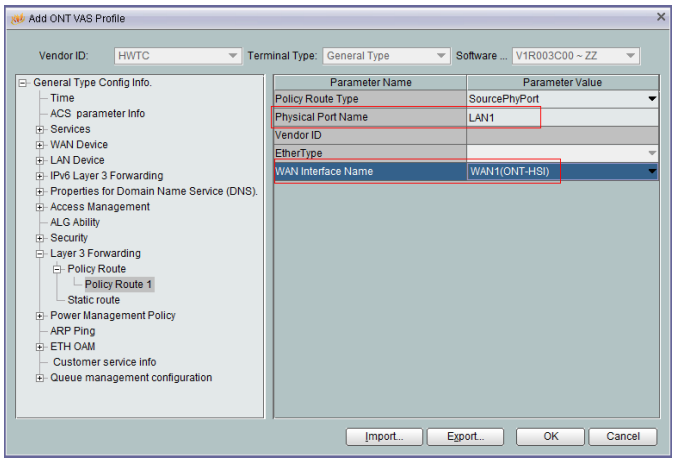
LAN port two three-port enable being **enable** indicates that the LAN port is a Layer 3 interface. The LAN port bound to the WAN port must be a Layer 3 interface.

b. Bind the LAN port to the WAN port.

1) In the navigation tree, choose **General Type Config Info** > **Layer 3 Forwarding** > **Policy Route**. Select **Policy Route**, right-click, and choose **Add** from the shortcut menu.

2) Select **Policy Route 1** and enter proper values.

- Policy Route Type: SourcePhyPort
- Physical Port Name: LAN1
- WAN Interface Name: WAN1(ONT-HSI)



Copyright © Huawei Technologies Co., Ltd.

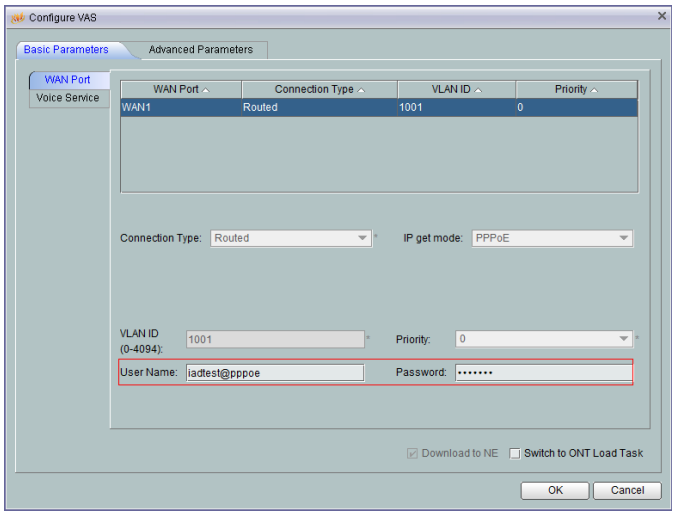
NOTE

To bind a LAN port to a WAN port, set **Physical Port Name** and **WAN Interface Name**. The preceding figure shows that WAN 1 is bound to LAN 1.

To bind a WAN port to multiple LAN ports, set **Physical Port Name** to **LAN1,...,LANx**. For example, to bind WAN 1 to LAN 1 and LAN 2, set **Physical Port Name** to **LAN1, LAN2**.

3) Click **OK**.

2. **Bind a general VAS profile.**
   a. In the Main Topology, double-click the required OLT in the **Physical Root** navigation tree; or right-click the required OLT and choose **NE Explorer** from the shortcut menu.
   b. Choose **GPON** > **GPON Management** from the navigation tree.
   c. In the window on the right, choose **GPON ONU**.
   d. On the **GPON ONU** tab page, set the filter criteria or click to display the GPON ONUs.
   e. Select an ONT from the list, right-click, and choose **Bind General VAS Profile** from the shortcut menu. In the dialog box that is displayed, select the created profile, and click **OK** to complete profile binding.
3. **Configure the ONT value-added service.**
   a. On the **GPON ONU** tab page, select an ONT, right-click, and choose **Configure Value-Added Service** from the shortcut menu.
   b. Click the **Basic Parameters** tab in the dialog box that is displayed, select **WAN Port**, set **User Name** to **iadtest@pppoe**, and set **Password** to **iadtest**. The user name and password must be the same as those configured on the BRAS.
   c. Click **OK**. The configurations take effect without the requirement of resetting the ONT.



----End

9.7.3.5 Configuring the H.248-based Voice Service (on a Web Page or the U2000)

The OLT is connected to the remote ONT through a GPON port to provide users with the IP-based high-quality and low-cost VoIP service.

Copyright © Huawei Technologies Co., Ltd.

Prerequisites

- The interface data and POTS user configuration data corresponding to the MG interface have been configured on the MGC.
- The OLT has been connected to the MGC. The OLT can ping the IP address of the MGC server successfully.
- The ONT has been added to the OLT. For details, see **9.7.1.3 Adding an ONT to an OLT**.
- Different voice services require different ONT software versions. Before the configuration, ensure that the current ONT software version supports H.248. For details, see relevant ONT manuals.

Context

Item	Data
ONT line profile	Profile name: ftth T-CONT ID: 4 GEM port ID: 12
VLAN Plan	Single VLAN tag: ● SVLAN ID: 200 ● SVLAN type: smart ● SVLAN attribute: common ● CVLAN ID: 300 VLAN translation policy: ● ONT: VLANs are configured for the ONTs on the same network in a unified manner, and the ONTs have the same C-VLAN. The ONT adds a C-VLAN tag to packets. ● OLT: translates the VLAN tag (C-VLAN <-> S-VLAN).
Voice parameter	IP address of the MGC server: 200.200.200.200/24 Port ID of the MGC server: 2944 MG Domain: 0100000001 or 0100000002

Procedure

- Configure the OLT.
  1. Configure a traffic profile.

     Run the **display traffic table ip** command to query the existing traffic profiles in the system. If the existing traffic profiles in the system do not meet the requirements, run the **traffic table ip** command to add a traffic profile.

     Set the profile name to **ftth_voip** and do not limit the upstream and downstream rates. Set the priority to **5** and packets are scheduled according to the priority carried.

Copyright © Huawei Technologies Co., Ltd.

```
huawei(config)#traffic table ip name ftth_voip cir off priority 5 priority-
policy
 local-setting
```

2. Configure the mapping relationship between a GEM port and a VLAN.

   The service flow of user VLAN 300 is mapped to GEM port 12 in the ONT line profile.

```
huawei(config)#ont-lineprofile gpon profile-name ftth
huawei(config-gpon-lineprofile-1)#gem mapping 12 2 vlan 300
huawei(config-gpon-lineprofile-1)#commit
huawei(config-gpon-lineprofile-1)#quit
```

3. Create a service VLAN and add an upstream port to it.

   Add upstream port 0/19/0 to VLAN 200.

```
huawei(config)#vlan 200 smart
huawei(config)#port vlan 200 0/19 0
```

4. Create service flows.

   Set the service VLAN to 200, GEM port ID to 12, and user VLAN to 300. Use traffic profile **ftth_voip**.

```
huawei(config)#service-port vlan 200 gpon 0/1/0 ont 1 gemport 12 multi-
service
user-vlan 300 inbound traffic-table name ftth_voip outboun
d traffic-table name ftth_voip
huawei(config)#service-port vlan 200 gpon 0/1/0 ont 2 gemport 12 multi-
service
user-vlan 300 inbound traffic-table name ftth_voip outboun
d traffic-table name ftth_voip
```

5. Enable the ARP proxy function.

   Voice media streams for different users of the same SVLAN fail to interchange because the service ports of the smart VLAN are isolated from each other. Therefore, the ARP proxy function needs to be enabled on the OLT.

```
huawei(config)#arp proxy enable
huawei(config)#interface vlanif 300
huawei(config-if-vlanif300)#arp proxy enable
huawei(config-if-vlanif300)#quit
```

6. Save the data.

```
huawei(config)#save
```

- Configure the ONT on the Web page.

  Log in to the Web page and then configure the ONT on the Web page.

  1. Configure the IP address of the PC network adapter to be in the same network segment with the IP address of the local maintenance Ethernet port on the ONT (default: 192.168.100.1).
  2. Open the Web browser, and enter the IP address (https://192.168.100.1:80 or http://192.168.100.1) (https with high priority is recommended) of the local maintenance Ethernet port on the ONT. In the login window that is displayed, enter the user name (default telecomadmin) and password (default admintelecom) of the administrator. After the password is authenticated, the web configuration window is displayed.

  NOTE

  The Web page for configuring ONT varies with ONT versions, but the parameter configuration is the same. For details, see relevant ONT manuals.

  1. Configure the voice protocol.

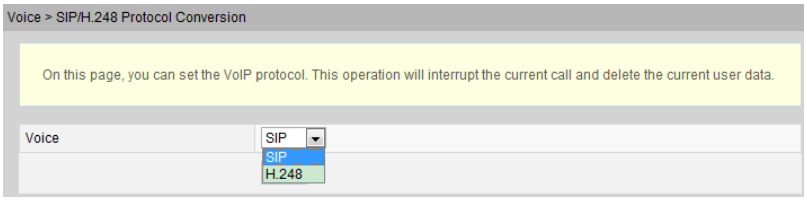
Copyright © Huawei Technologies Co., Ltd.

NOTE

The default voice protocol is SIP. Therefore, change the voice protocol first.

a. Choose **Voice** > **SIP/H.248 Protocol Conversion**.

b. In the pane on the right, set **Voice** to **H.248**.



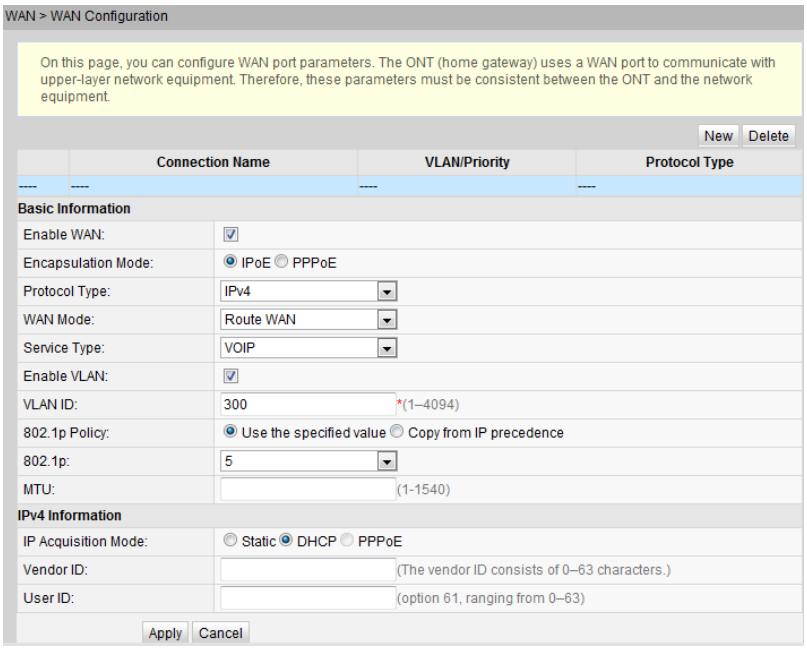
c. Click **Apply**.

2. Configure parameters for the voice WAN interface.

a. Choose **WAN** > **WAN Configuration**.

b. In the right pane, click **New**. In the dialog box that is displayed, set the parameters as follows:

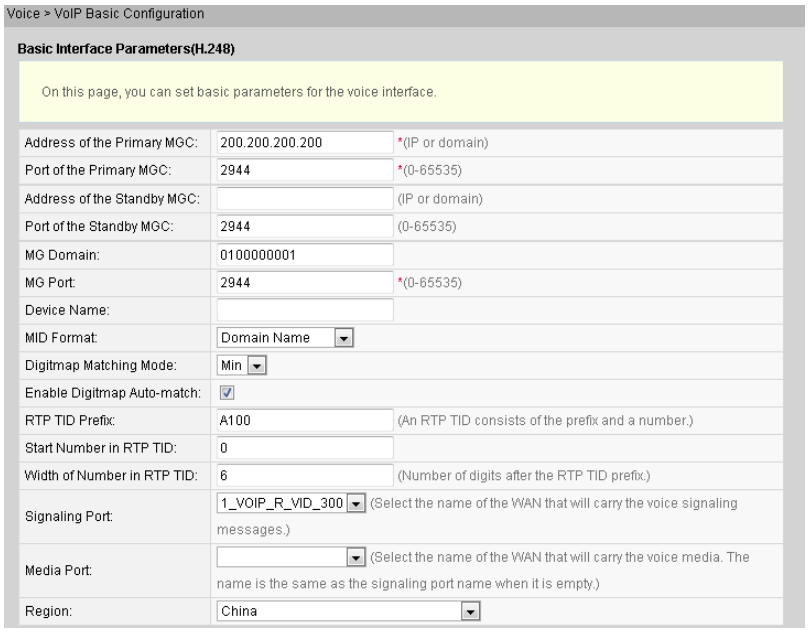
- Select **Enable WAN Connection** to enable the new WAN connection.
- Set **Encapsulation mode** to **IPoE**.
- Set **Service Type** to **VOIP**. (For configuring the VoIP service, VoIP or a combination containing VoIP needs to be selected.)
- Set **WAN mode** to **Route WAN**.
- Select **Enable VLAN**.
- Set **VLAN ID** to **300**. (The VLAN ID of the ONT must be the same as the user-side VLAN ID configured on the OLT.)
- Set **802.1p** to **5**.
- Set **IP Acquisition Mode** to **DHCP**.



c. Click **Apply**.

Copyright © Huawei Technologies Co., Ltd.

3. Configure parameters for the H.248-based voice interface.
   a. Choose **Voice** > **VoIP Basic Configuration**.
   b. In the **Basic Interface Parameters(H.248)** window, configure the parameters as follows:
      - Set **Address of the Primary MGC** to **200.200.200.200**.
      - Set **MID Format** to **Domain Name** and **MG Domain** to **0100000001**.
      - Set **Signaling Port** to **1_VOIP_R_VID_300**.
      - Set **Region** to **China**.



NOTE

- The parameters of the H.248-based voice interface must be consistent with the corresponding configuration on the media gateway controller (MGC).
- If dual-homing is configured, **Address of the Standby MGC** must be configured.
- **MID Format** can be set to **Domain Name**, **IP**, or **Device Name**. If **MID Format** is set to **Domain Name** or **Device Name**, the setting must be consistent with the corresponding configuration on the MGC.
- **MG Domain** is ONT's domain name registered with the MGC. It is globally unique. **MG Domain** in this example is ONT's password.
- If **Media Port** is empty, the parameter value is the same as **Signaling Port**. The media streams are not isolated from signaling streams. If the upper-layer network requires isolation of media streams from signaling streams, create different traffic streams for the media streams and signaling streams on the OLT, create different WAN ports on the ONT, and bind the created WAN ports to **Media Port** and **Signaling Port**. When the packet is forwarded from two WAN ports, the configured VLAN is carried by default.
- When the ONT is interconnected with a third-party softswitch, check **RTP TID Prefix**, **Start Number of RTP TID**, and **Width of RTP TID Number**.

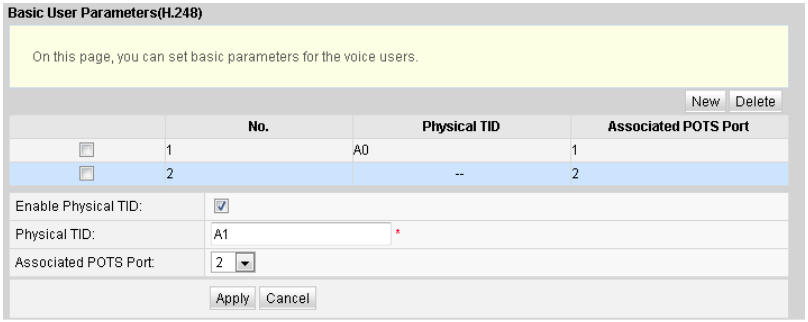
   c. Configure parameters for H.248-based voice users.
      a. Choose **Voice** > **VoIP Basic Configuration**.
      b. In the **Basic User Parameters(H.248)** window, set the parameters for user 1 as follows:

Copyright © Huawei Technologies Co., Ltd.

- Select **Enable Physical TID**.
- Set **Physical TID** to **A0**.
- Set **Associated POTS Port** to **1**.
- Click **Apply**.

Click **New** to add voice user 2, and set the parameters for voice user 2 as follows:

- Select **Enable Physical TID**.
- Set **Physical TID** to **A1**.
- Set **Associated POTS Port** to **2**.
- Click **Apply**.



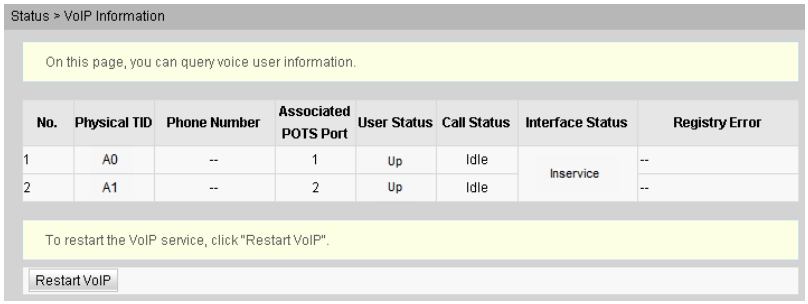
NOTE

- The terminal IDs **A0** and **A1** must be consistent with the corresponding configuration on the MGC.
- If **Associated POTS Port** is **1**, port TEL1 on the ONT is bound. If **Associated POTS Port** is **2**, port TEL2 on the ONT is bound.

d. Click **Apply**.

4. Check the registration status of the voice user.

   Choose **Status** > **VoIP Information**. In the right pane, **User Status** is **Up**.



- Configure the ONT on the U2000.

  NOTE

  The window for configuring ONT value-added service (VAS) profiles varies with ONT versions, but the parameter configuration is the same. For details, see relevant ONT manuals.

  1. **Configure a general VAS profile for the ONT.**

     a. From the main menu, choose **Configuration** > **Access Profile Management**. In the navigation tree of the tab page that is displayed, choose **PON Profile** > **ONT VAS Profile**.

Copyright © Huawei Technologies Co., Ltd.

b. On the **General ONT VAS Profile** tab page, right-click, and choose **Add** from the shortcut menu.

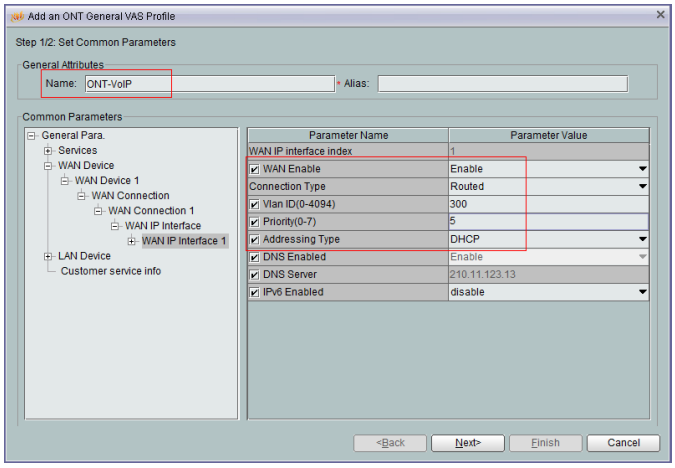
c. In the dialog box that is displayed, set **Name** to **ONT-VoIP**.

d. Configure the parameters of a voice WAN port.

   a. In the navigation tree, choose **General Para** > **WAN Device** > **WAN Device 1** > **WAN Connection**. Select **WAN Connection**, right-click, and choose **Add IP Connection** from the shortcut menu.

   b. Select **WAN IP Interface 1** and enter (or select) a proper value.

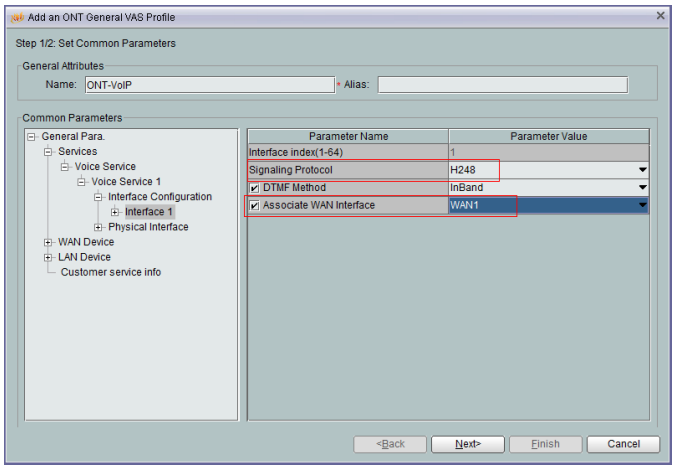
   - WAN Enable: enable
   - Connection Type: Routed
   - VLAN ID: 300 (The VLAN ID of the ONT must be the same as the user-side VLAN ID configured on the OLT.)
   - Priority: 5
   - Addressing Type: DHCP



e. Configure parameters of the voice protocol.

   In the navigation tree, choose **General Para** > **Services** > **Voice Service** > **Voice Service 1** > **Interface configuration** > **Interface 1**. Select **Interface 1** and select a proper value.

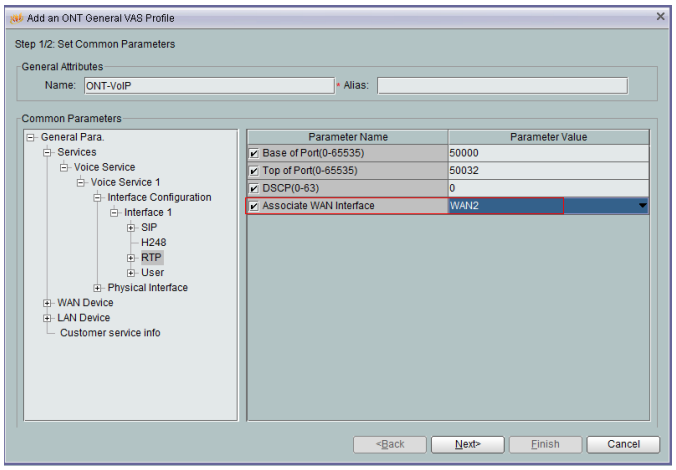
   - Signaling Protocol: H.248
   - Associate WAN Interface: WAN1 (binding the created voice WAN port)



Copyright © Huawei Technologies Co., Ltd.

NOTE

If the upper-layer network requires isolation of media streams from signaling streams, create different traffic streams for the media streams and signaling streams on the OLT. When the packet is forwarded from two WAN ports, the configured VLAN is carried by default. Create a WAN port named **WAN-RTP** on the ONT, and set this WAN port to a media WAN port. Specifically, choose **Interface 1** > **RTP** and set **Associate WAN Interface** to **WAN2**.



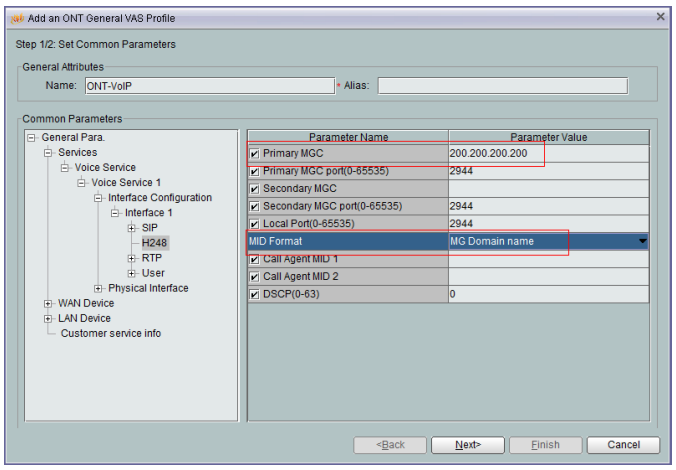
f. Configure the MGC parameters.

In the navigation tree, choose **General Para** > **Services** > **Voice Service** > **Voice Service 1** > **Interface configuration** > **Interface 1** > **H248**. Select **H248** and enter (or select) a proper value.

- Primary MGC: 200.200.200.200
- MID Format: MG Domain name

NOTE

- If dual-homing is configured, **Secondary MGC** must be set.
- **MID Format** can be set to **MG Domain Name**, **IP**, or **Device name**.



g. Configure the voice users.

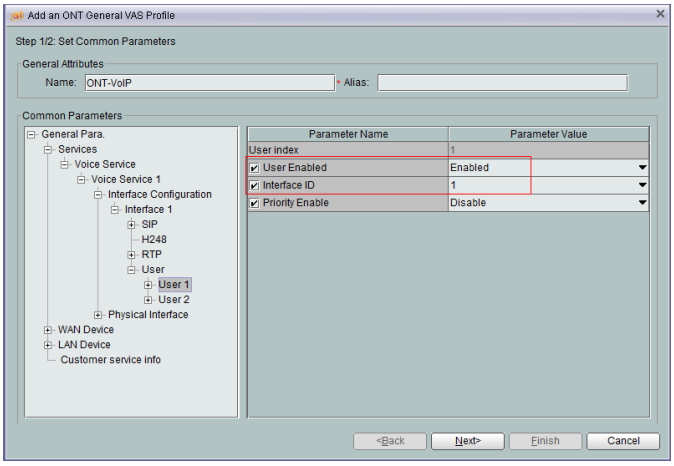
a. In the navigation tree, choose **General Para** > **Services** > **Voice Service** > **Voice Service 1** > **Interface configuration** > **Interface 1** > **User**. Right-click **User** and choose **Add** from the shortcut menu.

Copyright © Huawei Technologies Co., Ltd.

b. Select **User 1** under the **User** node. In the right pane, set **User Enabled** to **Enable**, and **Interface ID** to **1**. Then, select **User 2** under the **User** node. In the right pane, set **User Enabled** to **Enable**, and **Interface ID** to **2**.

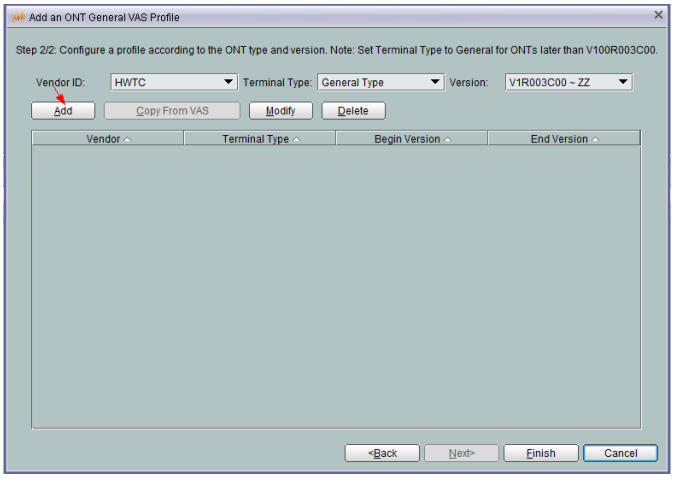
NOTE

If **Interface ID** is **1**, port TEL1 on the ONT is bound. If **Interface ID** is **2**, port TEL2 on the ONT is bound.



h. Click **Next**.

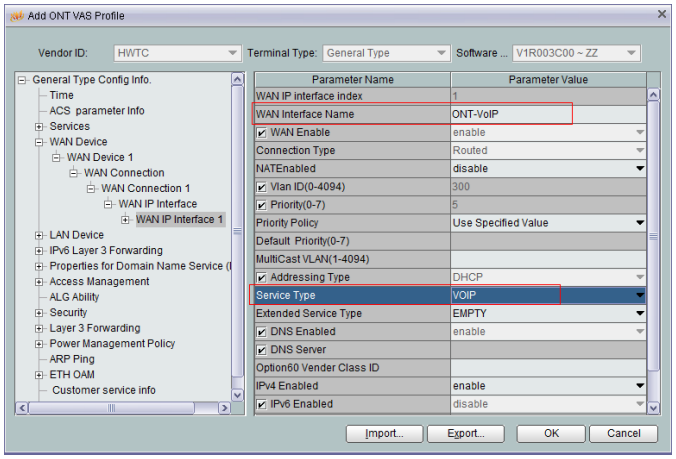
i. In the dialog box that is displayed, set **vendor ID** to **HWTC**, **Terminal Type** to **General Type**, and **Version** to **V1R003C00-ZZ**, click **Add**.



j. In the dialog box that is displayed, set the parameters.

- Choose **General Type Config Info** > **Services** > **Voice Service** > **Voice Service 1** > **Interface Configuration** > **Interface 1** from the navigation tree, and set **Region** to **China**.
- Choose **General Type Config Info** > **WAN Device** > **WAN Device 1** > **WAN Connection** > **WAN Connection 1** > **WAN IP Interface** > **WAN IP Interface 1** from the navigation tree, and set **WAN Interface Name** to **ONT-VoIP**, **Service Type** to **VOIP**.

Copyright © Huawei Technologies Co., Ltd.



k. Click **OK**.

2. **Bind a general VAS profile.**

   a. In the Main Topology, double-click the required OLT in the **Physical Root** navigation tree; or right-click the required OLT and choose **NE Explorer** from the shortcut menu.

   b. Choose **GPON** > **GPON Management** from the navigation tree.

   c. In the window on the right, choose **GPON ONU**.

   d. On the **GPON ONU** tab page, set the filter criteria or click to display the GPON ONUs.

   e. Select an ONT from the list, right-click, and choose **Bind General VAS Profile** from the shortcut menu. In the dialog box that is displayed, select the created profile, and click **OK** to complete profile binding.

3. **Configure the ONT VAS service.**

   a. On the **GPON ONU** tab page, select an ONT, right-click, and choose **Configure Value-Added Service** from the shortcut menu.

   b. Configure the domain name of the MG.

   Click the **Basic Parameters** tab in the dialog box that is displayed, select **Voice Service**, and set **MG Domain name** to **0100000001**.

   NOTE

   Domain Name is ONT's domain name registered with the MGC. It is globally unique. **MG Domain Name** in this example is ONT's password.

   c. Configure the terminal ID for the H.248 voice user.

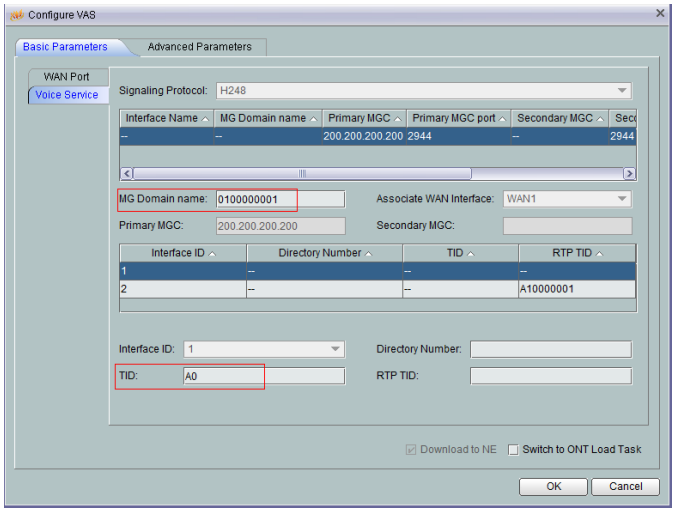
   Select the record where **Interface ID** is **1**, and set **TID** to **A0**. Select the record where **Interface ID** is **2**, and set **TID** to **A1**.

   NOTE

   Pay attention to the RTP TID configuration when the ONT is interconnected with a softswitch of other vendors. The terminal IDs **A0** and **A1** must be consistent with the corresponding configuration on the MGC.

   Do not configure **Directory Number**.

Copyright © Huawei Technologies Co., Ltd.



d. Click **OK**. The configurations take effect without the requirement of resetting the ONT.

----End

9.7.3.6 Configuring the H.248-based Voice Service (Through the CLI)

The OLT manages ONTs and applies VoIP configurations to the ONT using the OMCI protocol. This topic describes how to configure the H.248-based voice service.

Prerequisites

- The interface data and POTS user configuration data corresponding to the MG interface have been configured on the MGC.
- The OLT has been connected to the MGC. The OLT can ping the IP address of the MGC server successfully.
- The ONT has been added to the OLT. For details, see **9.7.1.3 Adding an ONT to an OLT**.
- Different voice services require different ONT software versions. Before the configuration, ensure that the current ONT software version supports H.248. For details, see relevant ONT manuals.
- The ONT software version of the H.248 voice service can be configured as V100R002C04 or later through the CLI.

Context

Item	Data
ONT line profile	Profile name: ftth T-CONT ID: 4 GEM port ID: 12

Copyright © Huawei Technologies Co., Ltd.

Item	Data
VLAN Plan	Single VLAN tag: ● SVLAN ID: 200 ● SVLAN type: smart ● SVLAN attribute: common ● CVLAN ID: 300 VLAN translation policy: ● ONT: VLANs are configured for the ONTs on the same network in a unified manner, and the ONTs have the same C-VLAN. The ONT adds a C-VLAN tag to packets. ● OLT: translates the VLAN tag (C-VLAN <-> S-VLAN).
Voice parameter	IP address of the MGC server: 200.200.200.200/24 Port ID of the MGC server: 2944 MG Domain: 0100000001 or 0100000002

Procedure

Step 1 Configure a traffic profile.

Run the **display traffic table ip** command to query the existing traffic profiles in the system. If the existing traffic profiles in the system do not meet the requirements, run the **traffic table ip** command to add a traffic profile.

Step 2 Configure the mapping relationship between a GEM port and a VLAN.

The service flow of user VLAN 300 is mapped to GEM port 12 in the ONT line profile.

```
huawei(config)#ont-lineprofile gpon profile-name ftth
huawei(config-gpon-lineprofile-1)#gem mapping 12 2 vlan 300
huawei(config-gpon-lineprofile-1)#commit
huawei(config-gpon-lineprofile-1)#quit
```

Step 3 Create a service VLAN and add an upstream port to it.

Add upstream port 0/19/0 to VLAN 200.

```
huawei(config)#vlan 200 smart
huawei(config)#port vlan 200 0/19 0
```

Step 4 Create service flows.

Set the service VLAN to 200, GEM port ID to 12, and user VLAN to 300. Use traffic profile **ftth_voip**.

```
huawei(config)#service-port vlan 200 gpon 0/1/0 ont 1 gemport 12 multi-service
user-vlan 300 inbound traffic-table name ftth_voip outboun
d traffic-table name ftth_voip
huawei(config)#service-port vlan 200 gpon 0/1/0 ont 2 gemport 12 multi-service
user-vlan 300 inbound traffic-table name ftth_voip outboun
d traffic-table name ftth_voip
```


Copyright © Huawei Technologies Co., Ltd.

Step 5 Configure the mode of issuing VoIP services.

Run the **ont voip config-method** command to configure the mode of issuing VoIP services. If the mode of issuing VoIP services is not **default** or **omci**, run this command to set the mode to **default** or **omci**. You can run the **display ont info** command to query the mode of issuing VoIP services.

In this example, the mode is **default**.

Step 6 Configure ONT voice service profiles.

ONT voice service profiles include the interface common profile, MGC interface profile, and POTS port profile.

- Interface common profile: saves common attributes of an ONT voice interface, including the fax mode, fax/modem negotiation mode, and priority of the coding and decoding mode.
- MGC interface profile: saves the IP address or domain name of the MGC, protocol port ID of the MGC transport layer to which the MG interface belongs, and DSCP priority of media packets.
- POTS port profile: saves physical attributes of a POTS port on an ONT, including the impedance, transmitting gain, receiving gain, and signaling type of the POTS port.

1. Configure an interface common profile.

   Run the **display ont-mg-attribute-profile** command to query the existing interface common profile in the system. If the existing interface common profile in the system does not meet the requirements, run the **ont-mg-attribute-profile add** command to add an interface common profile.

   In this example, the default interface common profile, namely interface common profile 1 is used.

2. Configure an MGC interface profile.

   Run the **display ont-mgc-profile** command to query the existing MGC interface profile in the system. If the existing MGC interface profile in the system does not meet the requirements, run the **ont-mgc-profile add** command to add an MGC interface profile.

   Create MGC interface profile 2, set the IP address of the MGC to 200.200.200.200, and use default values for other parameters.

   ```
   huawei(config)#ont-mgc-profile add profile-id 2 primary-mgc 200.200.200.200
   ```

3. Configure a POTS port profile.

   Run the **display ont-pots-profile** command to query the existing POTS port profile in the system. If the existing POTS port profile in the system does not meet the requirements, run the **ont-pots-profile add** command to add a POTS port profile.

   In this example, the default POTS port profile, namely POTS port profile 1 is used.

Step 7 Configure the IP addresses of ONT SIP users.

For ONT 1 and ONT 2, configure the IP address obtaining mode to DHCP mode, set the management VLAN to VLAN 20, and use default values for other parameters.

```
huawei(config)#interface gpon 0/1
huawei(config-if-gpon-0/1)#ont ipconfig 0 1 dhcp vlan 20
huawei(config-if-gpon-0/1)#ont ipconfig 0 2 dhcp vlan 20
```

Step 8 Configure H.248 POTS users.

1. Add an H.248 interface and apply an MGC interface profile to the interface.

   For ONT 1 and ONT 2, set the MG ID to 1, apply MGC interface profile 2 to ONT 1 and ONT 2, and use default values for other parameters.

Copyright © Huawei Technologies Co., Ltd.

If parameters of an MGC interface profile are changed, the MGC interface profile must be reapplied to the ONT so that the changed parameters can take effect.

```
huawei(config-if-gpon-0/1)#if-h248 add 0 1 1 mgc-profile profile-id 2
huawei(config-if-gpon-0/1)#if-h248 add 0 2 1 mgc-profile profile-id 2
```

2. Add POTS users.

   For ONT 1 and ONT 2, create a POTS user, set the MG ID to 1 (identical to the MG ID of the H.248 interface), and set the physical terminal port ID to A0 and A1.

```
huawei(config-if-gpon-0/1)#mgpstnuser add 0 1 1 mgid 1 terminalid A0
huawei(config-if-gpon-0/1)#mgpstnuser add 0 2 1 mgid 1 terminalid A1
```

   Run the **display mgpstnuser attribute** command to check whether the configuration of the POTS user is properly set.

```
huawei(config-if-gpon-0/1)#display mgpstnuser attribute 0 1 1

-------------------------------------------------------------------------------
  F/S/P                       : 0/1/0
  ONT ID                      : 1
  Port ID                     : 1

  MG ID                       : 1
  Terminal ID                 : A0
...//The rest of the response information is omitted.

huawei(config-if-gpon-0/1)#display mgpstnuser attribute 0 2 1

-------------------------------------------------------------------------------
  F/S/P                       : 0/1/0
  ONT ID                      : 2
  Port ID                     : 1

  MG ID                       : 1
  Terminal ID                 : A1
...//The rest of the response information is omitted.
```

Step 9 Apply ONT voice service profiles

After ONT voice service profiles are applied, if parameters in those profiles are changed, those profiles must be reapplied so that the changed parameters can take effect.

1. Apply an interface common profile.

   Run the **if-h248 attribute** command to apply an interface common profile to an H.248 interface or configure the interface customized parameters, or run the **ont-if-h248 bat-apply** command to bulk apply the interface common profiles to H.248 interfaces. If you use these two commands to apply the interface common profiles or configure the interface customized parameters repeatedly, the last configurations take effect.

   In this example, the default interface common profile, namely interface common profile 1 is used.

2. Apply a POTS port profile.

   Run the **pstnport electric** command to apply a POTS port profile to an H.248 interface or configure the interface customized parameters, or run the **ont-pstnport electric bat-apply** command to bulk apply the POTS port profiles to H.248 interfaces. If you use these two commands to apply the POTS port profiles or configure the interface customized parameters repeatedly, the last configurations take effect.

   In this example, the default POTS port profile, namely POTS port profile 1 is used.

Step 10 (Optional) Configure the H.248 user codec.

Copyright © Huawei Technologies Co., Ltd.

Run the **mgpstnuser codec** command to configure the H.248 user codec. The H.248 user codec will not be configured independently in this example.

Step 11 Save the data.

```
huawei(config)#save
```

----End

9.7.3.7 Configuring the SIP-based Voice Service (on a Web Page or the U2000)

The OLT is connected to the remote ONT through a GPON port to provide users with the IP-based high-quality and low-cost VoIP service.

Prerequisites

- The SIP interface data and POTS user configuration data corresponding to the MG interface have been configured on the SIP server.
- The connection between the OLT and the SIP server is set up. The OLT can ping the IP address of the SIP server successfully.
- The ONT has been added to the OLT. For details, see **9.7.1.3 Adding an ONT to an OLT**.
- Different voice services require different ONT software versions. Before the configuration, ensure that the current ONT software version supports SIP. For details, see relevant ONT manuals.

Data Plan

Item	Data
ONT line profile	Profile name: ftth T-CONT ID: 4 GEM port ID: 12
VLAN Plan	Single VLAN tag: ● SVLAN ID: 200 ● SVLAN type: smart ● SVLAN attribute: common ● CVLAN ID: 300 VLAN translation policy: ● ONT: VLANs are configured for the ONTs on the same network in a unified manner, and the ONTs have the same C-VLAN. The ONT adds a C-VLAN tag to packets. ● OLT: translates the VLAN tag (C-VLAN <-> S-VLAN).

Copyright © Huawei Technologies Co., Ltd.

Item	Data
Voice parameter	IP address of the SIP server: 200.200.200.200/24 Port ID of the SIP server: 5060 Home domain name: huawei.com User phone number 1: 77730010 User phone number 2: 77730020

Procedure

- Configure the OLT.
  1. Configure a traffic profile.

     Run the **display traffic table ip** command to query the existing traffic profiles in the system. If the existing traffic profiles in the system do not meet the requirements, run the **traffic table ip** command to add a traffic profile.

     Set the profile name to **ftth_voip** and do not limit the upstream and downstream rates. Set the priority to **5** and packets are scheduled according to the priority carried.

     ```
     huawei(config)#traffic table ip name ftth_voip cir off priority 5 priority-policy
      local-setting
     ```

  2. Configure the mapping relationship between a GEM port and a VLAN.

     The service flow of user VLAN 300 is mapped to GEM port 12 in the ONT line profile.

     ```
     huawei(config)#ont-lineprofile gpon profile-name ftth
     huawei(config-gpon-lineprofile-1)#gem mapping 12 2 vlan 300
     huawei(config-gpon-lineprofile-1)#commit
     huawei(config-gpon-lineprofile-1)#quit
     ```

  3. Create a service VLAN and add an upstream port to it.

     Add upstream port 0/19/0 to VLAN 200.

     ```
     huawei(config)#vlan 200 smart
     huawei(config)#port vlan 200 0/19 0
     ```

  4. Create service flows.

     Set the service VLAN to 200, GEM port ID to 12, and user VLAN to 300. Use traffic profile **ftth_voip**.

     ```
     huawei(config)#service-port vlan 200 gpon 0/1/0 ont 1 gemport 12 multi-service
     user-vlan 300 inbound traffic-table name ftth_voip outboun
     d traffic-table name ftth_voip
     huawei(config)#service-port vlan 200 gpon 0/1/0 ont 2 gemport 12 multi-service
     user-vlan 300 inbound traffic-table name ftth_voip outboun
     d traffic-table name ftth_voip
     ```

  5. Enable the ARP proxy function.

     Voice media streams for different users of the same SVLAN fail to interchange because the service ports of the smart VLAN are isolated from each other. Therefore, the ARP proxy function needs to be enabled on the OLT.

     ```
     huawei(config)#arp proxy enable
     huawei(config)#interface vlanif 300
     ```


Copyright © Huawei Technologies Co., Ltd.

```
huawei(config-if-vlanif300)#arp proxy enable
huawei(config-if-vlanif300)#quit
```

6. Save the data.

```
huawei(config)#save
```

- Configure the ONT on the Web page.

  Log in to the Web page and then configure the ONT on the Web page.

  1. Configure the IP address of the PC network adapter to be in the same network segment with the IP address of the local maintenance Ethernet port on the ONT (default: 192.168.100.1).
  2. Open the Web browser, and enter the IP address (https://192.168.100.1:80 or http://192.168.100.1) (https with high priority is recommended) of the local maintenance Ethernet port on the ONT. In the login window that is displayed, enter the user name (default telecomadmin) and password (default admintelecom) of the administrator. After the password is authenticated, the web configuration window is displayed.

  NOTE

  The Web page for configuring ONT varies with ONT versions, but the parameter configuration is the same. For details, see relevant ONT manuals.

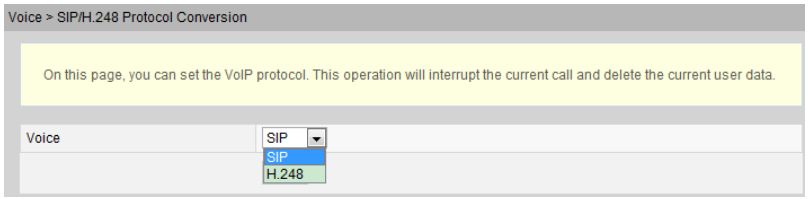
  1. **Optional:** Configure the voice protocol.

     NOTE

     The default voice protocol is SIP. If the protocol is not changed, skip this step.

     a. Choose **Voice** > **SIP/H.248 Protocol Conversion**.

     b. In the pane on the right, set **Voice** to **SIP**.

     c. Click **Apply**.

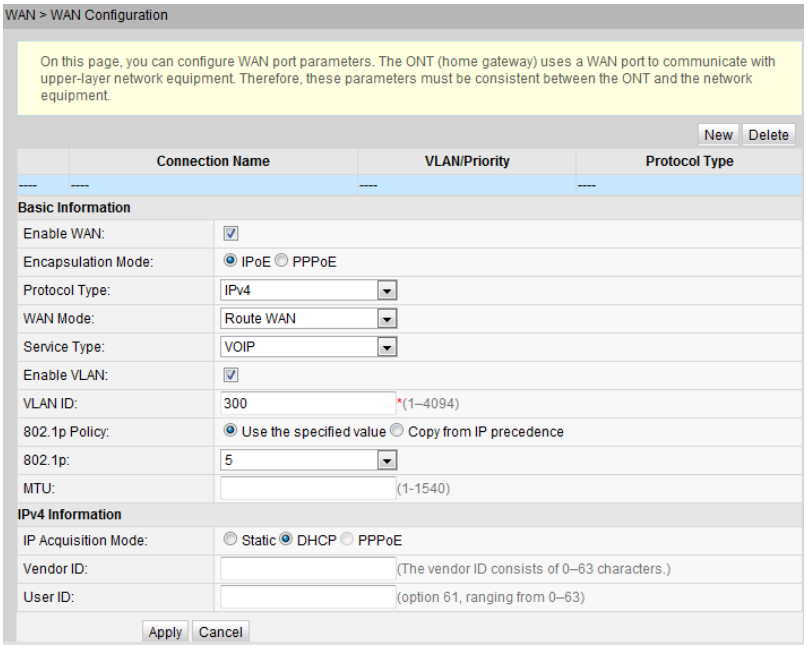
  2. Configure parameters for the voice WAN interface.

     a. Choose **WAN** > **WAN Configuration**.

     b. In the right pane, click **New**. In the dialog box that is displayed, set the parameters as follows:

        - Select **Enable WAN Connection** to enable the new WAN connection.
        - Set **Encapsulation mode** to **IPoE**.
        - Set **Service Type** to **VOIP**. (For configuring the VoIP service, VoIP or a combination containing VoIP needs to be selected.)
        - Set **WAN mode** to **Route WAN**.
        - Select **Enable VLAN**.
        - Set **VLAN ID** to **300**. (The VLAN ID of the ONT must be the same as the user-side VLAN ID configured on the OLT.)
        - Set **802.1p** to **5**.
        - Set **IP Acquisition Mode** to **DHCP**.

Copyright © Huawei Technologies Co., Ltd.



c. Click **Apply**.

3. Configure parameters for the SIP-based voice interface.

a. Choose **Voice** > **VoIP Basic Configuration**.

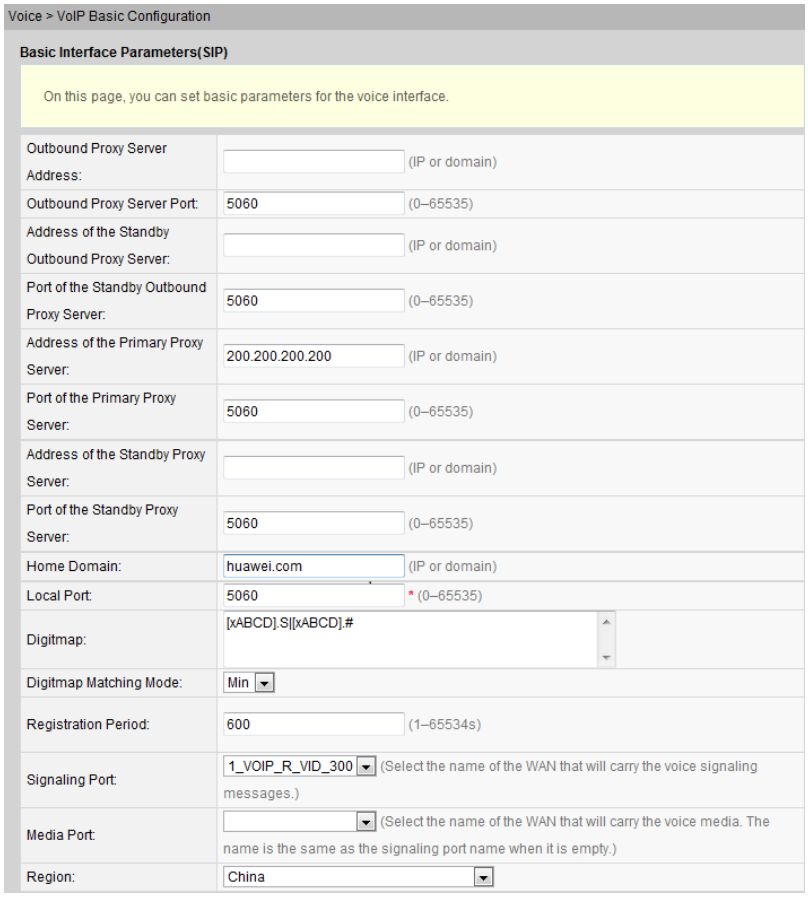
b. In the **Basic Interface Parameters(SIP)** window, configure the parameters as follows:

- Set **Address of the Primary Proxy Server** to **200.200.200.200**.
- Set **Home Domain** to **huawei.com**.
- Set **Region** to **China**.
- Set **Signaling Port** to **1_VOIP_R_VID_300**.

NOTE

- The parameters of the SIP-based voice interface must be consistent with the corresponding configuration on the softswitch.
- If dual-homing is configured, **Address of the Standby Proxy Server** must be configured.
- If **Signaling Port** is empty, the parameter value is the same as **Media Port**. If the upper-layer network requires isolation of media streams from signaling streams, create different traffic streams for the media streams and signaling streams on the OLT, create different WAN ports on the ONT, and bind the created WAN ports to **Media Port** and **Signaling Port**. When the packet is forwarded from two WAN ports, the configured VLAN is carried by default.

Copyright © Huawei Technologies Co., Ltd.



c. Configure parameters for the SIP-based voice users.

a. Choose **Voice** > **VoIP Basic Configuration**.

b. In the **Basic User Parameters(SIP)** window, set parameters for voice user 1 as follows:

- Select **Enable User** to enable the voice user configuration.
- Set **Registration User Name** to **77730010**.
- Set **Associated POTS Port** to **1**.
- Set **Authentication User Name** to **+8675577730010@huawei.com**.
- Set **Password** to **iadtest1**.

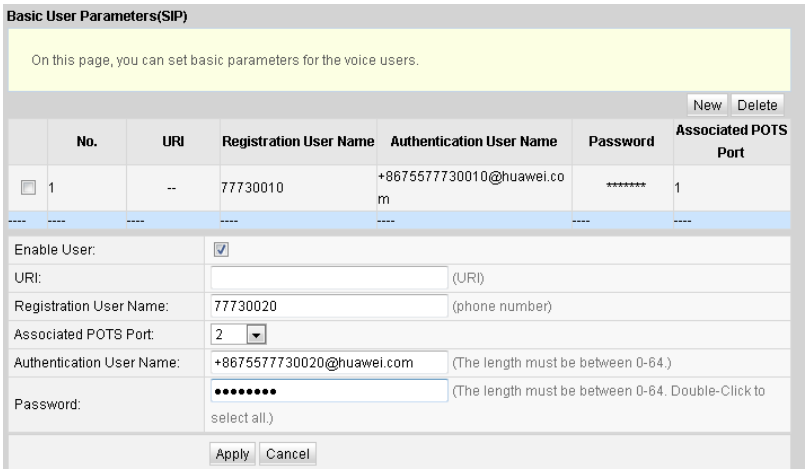
Click **New** to add voice user 2, and set the parameters for voice user 2 as follows:

- Select **Enable User** to enable the voice user configuration.
- Set **Registration User Name** to **77730020**.
- Set **Associated POTS Port** to **2**.
- Set **Authentication User Name** to **+8675577730020@huawei.com**.
- Set **Password** to **iadtest2**.

Copyright © Huawei Technologies Co., Ltd.

NOTE

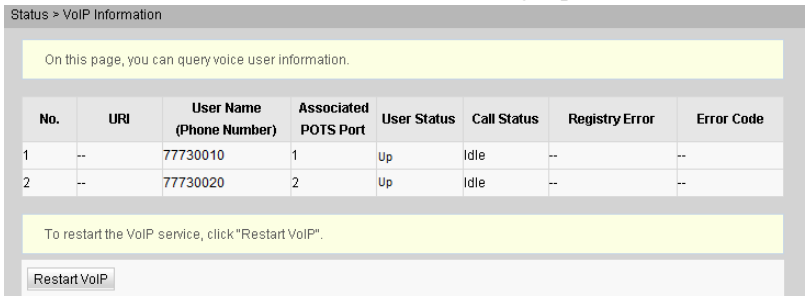
- The parameters of the SIP-based voice user must be consistent with the corresponding configuration on the softswitch.
- If **Associated POTS Port** is **1**, port TEL1 on the ONT is bound. If **Associated POTS Port** is **2**, port TEL2 on the ONT is bound.



d. Click **Apply**.

4. Check the registration status of the voice user.

   Choose **Status** > **VoIP Information**. In the right pane, **User Status** is **Up**.



- Configure the ONT on the U2000.

  NOTE

  The window for configuring ONT value-added service (VAS) profiles varies with ONT versions, but the parameter configuration is the same. For details, see relevant ONT manuals.

  1. Configure a general VAS profile for the ONT.

     a. From the main menu, choose **Configuration** > **Access Profile Management**. In the navigation tree of the tab page that is displayed, choose **PON Profile** > **ONT VAS Profile**.

     b. On the **General ONT VAS Profile** tab page, right-click, and choose **Add** from the shortcut menu.

     c. In the dialog box that is displayed, set **Name** to **ONT-VoIP**.

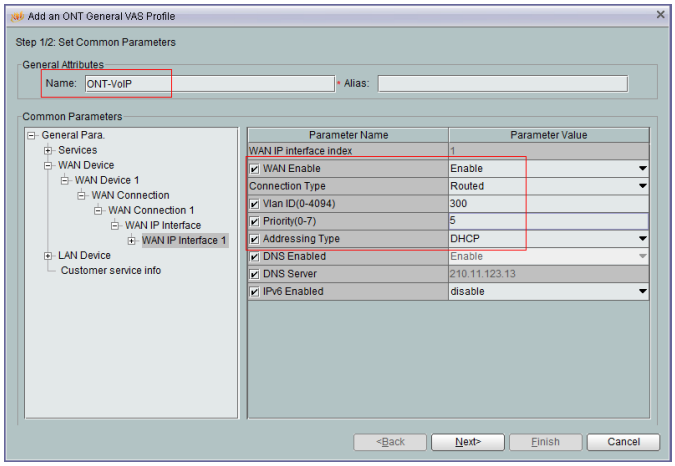
     d. Configure the parameters of a voice WAN port.

        a. In the navigation tree, choose **General Para** > **WAN Device** > **WAN Device 1** > **WAN Connection**. Select **WAN Connection**, right-click, and choose **Add IP Connection** from the shortcut menu.

        b. Select **WAN IP Interface 1** and enter (or select) a proper value.

Copyright © Huawei Technologies Co., Ltd.

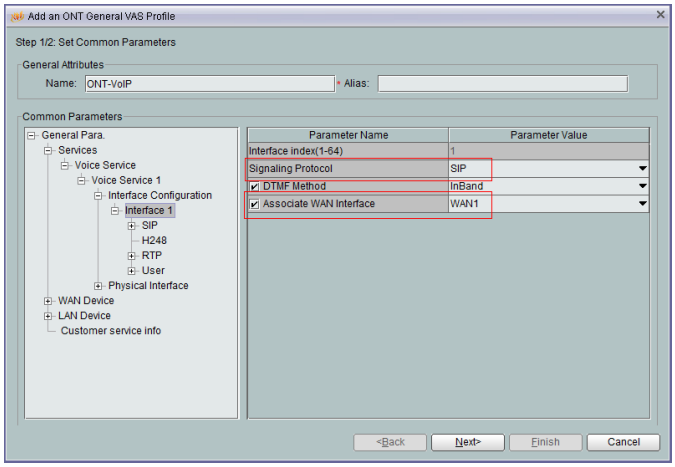
- WAN Enable: enable
- Connection Type: Routed
- VLAN ID: 300 (The VLAN ID of the ONT must be the same as the user-side VLAN ID configured on the OLT.)
- Priority: 5
- Addressing Type: DHCP



e. Configure parameters of the voice protocol.

In the navigation tree, choose **General Para** > **Services** > **Voice Service** > **Voice Service 1** > **Interface configuration** > **Interface 1**. Select **Interface 1** and select a proper value.

- Signaling Protocol: SIP
- Associate WAN Interface: WAN1 (binding the created voice WAN port)



f. Configure SIP protocol parameters.

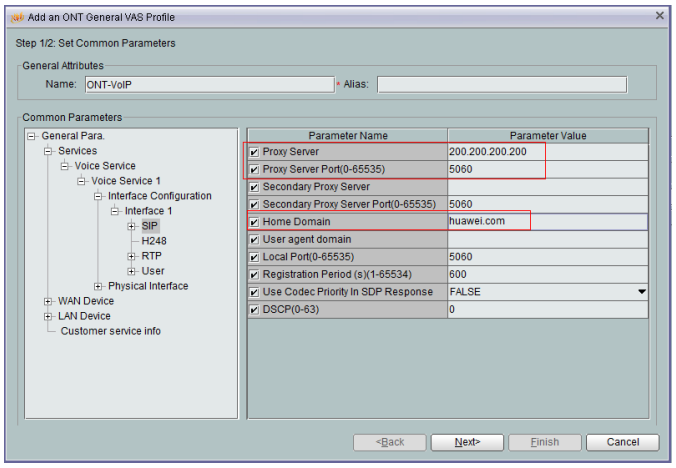
In the navigation tree, choose **General Para** > **Services** > **Voice Service** > **Voice Service 1** > **Interface configuration** > **Interface 1** > **SIP**. Select **SIP** and enter (or select) a proper value.

- Proxy Server: 200.200.200.200
- Server Port: 5060
- Home Domain: huawei.com

Copyright © Huawei Technologies Co., Ltd.

NOTE

If dual-homing is configured, **Secondary Proxy Server** must be set.



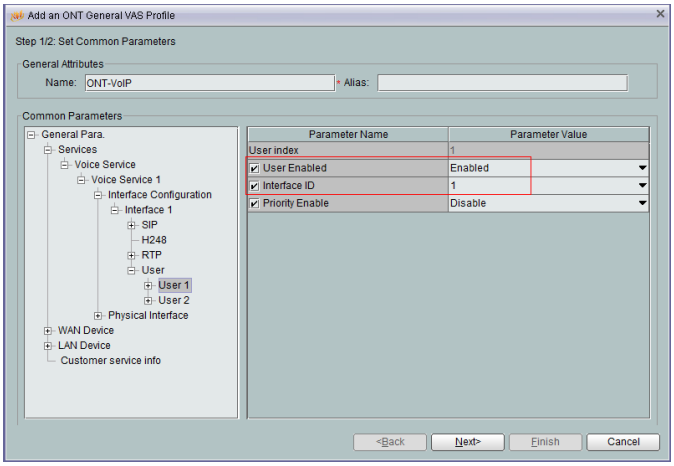
g. Configure the voice users.

a. In the navigation tree, choose **General Para** > **Services** > **Voice Service** > **Voice Service 1** > **Interface configuration** > **Interface 1** > **User**. Right-click **User** and choose **Add** from the shortcut menu.

b. Select **User 1** under the **User** node. In the right pane, set **User Enabled** to **Enable**, and **Interface ID** to **1**. Then, select **User 2** under the **User** node. In the right pane, set **User Enabled** to **Enable**, and **Interface ID** to **2**.

NOTE

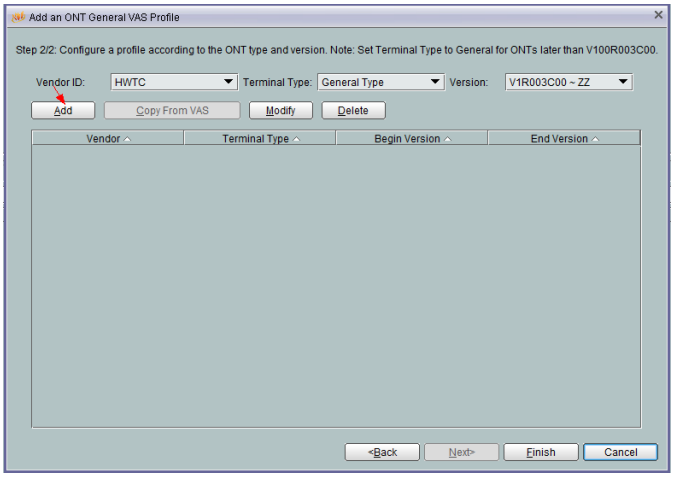
If **Interface ID** is **1**, port TEL1 on the ONT is bound. If **Interface ID** is **2**, port TEL2 on the ONT is bound.



h. Click **Next**.

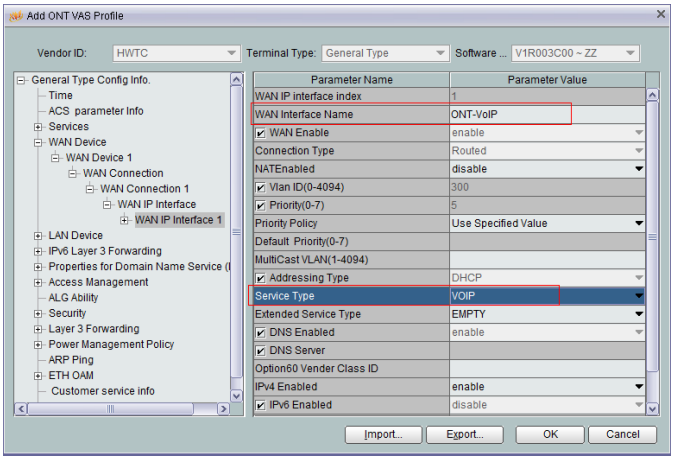
i. In the dialog box that is displayed, set **vendor ID** to **HWTC**, **Terminal Type** to **General Type**, and **Version** to **V1R003C00-ZZ**, click **Add**.

Copyright © Huawei Technologies Co., Ltd.



j. In the dialog box that is displayed, set the parameters.

- Choose **General Type Config Info** > **Services** > **Voice Service** > **Voice Service 1** > **Interface Configuration** > **Interface 1** from the navigation tree, and set **Region** to **China**.
- Choose **General Type Config Info** > **WAN Device** > **WAN Device 1** > **WAN Connection** > **WAN Connection 1** > **WAN IP Interface** > **WAN IP Interface 1** from the navigation tree, and set **WAN Interface Name** to **ONT-VoIP**, **Service Type** to **VOIP**.



k. Click **OK**.

2. **Bind a general VAS profile.**

a. In the Main Topology, double-click the required OLT in the **Physical Root** navigation tree; or right-click the required OLT and choose **NE Explorer** from the shortcut menu.

b. Choose **GPON** > **GPON Management** from the navigation tree.

c. In the window on the right, choose **GPON ONU**.

d. On the **GPON ONU** tab page, set the filter criteria or click to display the GPON ONUs.

e. Select an ONT from the list, right-click, and choose **Bind General VAS Profile** from the shortcut menu. In the dialog box that is displayed, select the created profile, and click **OK** to complete profile binding.

Copyright © Huawei Technologies Co., Ltd.

3. **Configure the ONT VAS service.**

   a. On the **GPON ONU** tab page, select an ONT, right-click, and choose **Configure Value-Added Service** from the shortcut menu.

   b. Configure parameters for the SIP-based voice users.

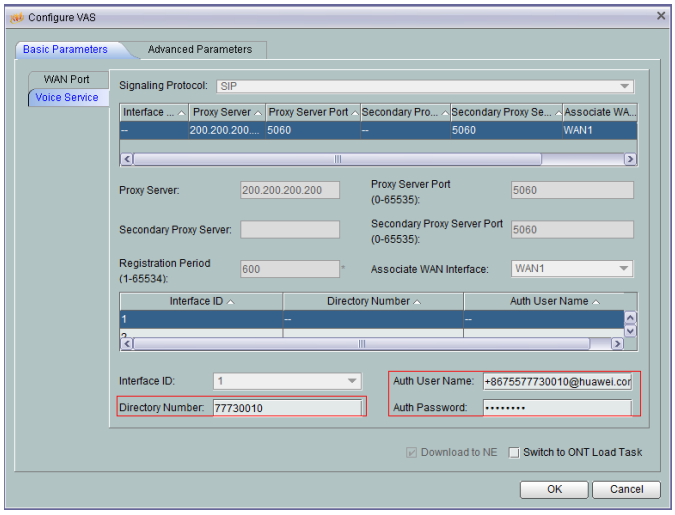
   NOTE

   The parameters of the SIP-based voice user must be consistent with the corresponding configuration on the softswitch.

      a. Click the **Basic Parameters** tab in the dialog box that is displayed, select **Voice Service**. Select **User 1** and set **Directory Number** to **77730010**.

      b. Select **SIP** below **User 1** and enter a proper value.

         - Auth User Name: +8675577730010@huawei.com
         - Auth Password: iadtest1



      c. Set parameters of **User 2** using the same method.

         - Directory Number: 77730020
         - Auth User Name: +8675577730020@huawei.com
         - Auth Password: iadtest2

   c. Click **OK**. The configurations take effect without the requirement of resetting the ONT.

----End

9.7.3.8 Configuring the SIP-based Voice Service (Through the CLI)

The OLT manages ONTs and applies VoIP configurations to the ONT using the OMCI protocol. This topic describes how to configure the SIP-based voice service.

Prerequisites

- The SIP interface data and POTS user configuration data corresponding to the MG interface have been configured on the SIP server.
- The connection between the OLT and the SIP server is set up. The OLT can ping the IP address of the SIP server successfully.

Copyright © Huawei Technologies Co., Ltd.

- The ONT has been added to the OLT. For details, see **9.7.1.3 Adding an ONT to an OLT**.
- Different voice services require different ONT software versions. Before the configuration, ensure that the current ONT software version supports SIP. For details, see relevant ONT manuals.
- The ONT software version of the SIP voice service can be configured as V100R002C04 or later through the CLI.

Data Plan

Item	Data
ONT line profile	Profile name: ftth T-CONT ID: 4 GEM port ID: 12
VLAN Plan	Single VLAN tag: ● SVLAN ID: 200 ● SVLAN type: smart ● SVLAN attribute: common ● CVLAN ID: 300 VLAN translation policy: ● ONT: VLANs are configured for the ONTs on the same network in a unified manner, and the ONTs have the same C-VLAN. The ONT adds a C-VLAN tag to packets. ● OLT: translates the VLAN tag (C-VLAN <-> S-VLAN).
Voice parameter	IP address of the SIP server: 200.200.200.200/24 Port ID of the SIP server: 5060 Home domain name: huawei.com User phone number 1: 77730010 User phone number 2: 77730020

Procedure

Step 1 Configure a traffic profile.

Run the **display traffic table ip** command to query the existing traffic profiles in the system. If the existing traffic profiles in the system do not meet the requirements, run the **traffic table ip** command to add a traffic profile.

Step 2 Configure the mapping relationship between a GEM port and a VLAN.

The service flow of user VLAN 300 is mapped to GEM port 12 in the ONT line profile.

```
huawei(config)#ont-lineprofile gpon profile-name ftth
huawei(config-gpon-lineprofile-1)#gem mapping 12 2 vlan 300
```


Copyright © Huawei Technologies Co., Ltd.

```
huawei(config-gpon-lineprofile-1)#commit
huawei(config-gpon-lineprofile-1)#quit
```

Step 3 Create a service VLAN and add an upstream port to it.

Add upstream port 0/19/0 to VLAN 200.

```
huawei(config)#vlan 200 smart
huawei(config)#port vlan 200 0/19 0
```

Step 4 Create service flows.

Set the service VLAN to 200, GEM port ID to 12, and user VLAN to 300. Use traffic profile **ftth_voip**.

```
huawei(config)#service-port vlan 200 gpon 0/1/0 ont 1 gemport 12 multi-service
user-vlan 300 inbound traffic-table name ftth_voip outboun
d traffic-table name ftth_voip
huawei(config)#service-port vlan 200 gpon 0/1/0 ont 2 gemport 12 multi-service
user-vlan 300 inbound traffic-table name ftth_voip outboun
d traffic-table name ftth_voip
```

Step 5 Configure the mode of issuing VoIP services.

Run the **ont voip config-method** command to configure the mode of issuing VoIP services. If the mode of issuing VoIP services is not **default** or **omci**, run this command to set the mode to **default** or **omci**. You can run the **display ont info** command to query the mode of issuing VoIP services.

In this example, the mode is **default**.

Step 6 Configure ONT voice service profiles.

ONT voice service profiles include the interface common profile, SIP agent profile, SIP service data profile, POTS port profile, and digitmap profile.

- Interface common profile: saves common attributes of an ONT voice interface, including the fax mode, fax/modem negotiation mode, and priority of the coding and decoding mode.
- SIP agent profile: saves the SIP agent information about an ONT, including the IP address and domain name of the SIP agent server and attributes of media packets and signaling packets.
- SIP service data profile: saves the data information about ONT voice services, including the rights of the call waiting service, three-party service, call forwarding service, and call holding service.
- POTS port profile: saves physical attributes of a POTS port on an ONT, including the impedance, transmitting gain, receiving gain, and signaling type of the POTS port.
- Digitmap profile: saves the digitmap information about an ONT, including the timeout time of the digitmap timer and the digitmap format.

1. Configure an interface common profile.

   Run the **display ont-mg-attribute-profile** command to query the existing interface common profile in the system. If the existing interface common profile in the system does not meet the requirements, run the **ont-mg-attribute-profile add** command to add an interface common profile.

   In this example, the default interface common profile, namely interface common profile 1 is used.

2. Configure an SIP agent profile.

Copyright © Huawei Technologies Co., Ltd.

Run the **display ont-sipagent-profile** command to query the existing SIP agent profile in the system. If the existing SIP agent profile in the system does not meet the requirements, run the **ont-sipagent-profile add** command to add an SIP agent profile.

Create SIP agent profile 2, set the IP address of the SIP server to 200.200.200.200, and use default values for other parameters.

```
huawei(config)#ont-sipagent-profile add profile-id 2 proxy-server
200.200.200.200
```

3. Configure an SIP service data profile.

   Run the **display ont-siprightflag-profile** command to query the existing SIP agent profile in the system. If the existing SIP service data profile in the system does not meet the requirements, run the **ont-siprightflag-profile add** command to add an SIP service data profile.

   In this example, the default SIP service data profile, namely SIP service data profile 1 is used.

4. Configure a POTS port profile.

   Run the **display ont-pots-profile** command to query the existing POTS port profile in the system. If the existing POTS port profile in the system does not meet the requirements, run the **ont-pots-profile add** command to add a POTS port profile.

   In this example, the default POTS port profile, namely POTS port profile 1 is used.

5. Configure a digitmap profile.

   Run the **display ont-digitmap-profile** command to query the existing digitmap profile in the system. If the existing digitmap profile in the system does not meet the requirements, run the **ont-digitmap-profile add** command to add a digitmap profile.

   In this example, the default digitmap profile, namely digitmap profile 1 is used.

Step 7 Configure an IP address for an ONT SIP user.

For ONT 1 and ONT 2, configure the IP address obtaining mode to the DHCP mode, set the management VLAN to VLAN 20, and use default values for other parameters.

```
huawei(config)#interface gpon 0/1
huawei(config-if-gpon-0/1)#ont ipconfig 0 1 dhcp vlan 20
huawei(config-if-gpon-0/1)#ont ipconfig 0 2 dhcp vlan 20
```

Step 8 Configure SIP POTS users.

1. Add an SIP interface and apply an SIP agent profile to the interface.

   For ONT 1 and ONT 2, set the MG ID to 1, apply SIP agent profile 2 to ONT 1 and ONT 2, and use default values for other parameters.

   If parameters in an SIP agent profile are changed, the SIP agent profile must be reapplied to the ONT so that the changed parameters can take effect.

   ```
   huawei(config-if-gpon-0/1)#if-sip add 0 1 1 sipagent-profile profile-id 2
   huawei(config-if-gpon-0/1)#if-sip add 0 2 1 sipagent-profile profile-id 2
   ```

2. Add POTS users.

   For ONT 1 and ONT 2, set the MG ID to 1 (identical to the MG ID of the added SIP interface), create two POTS users named huawei1 and huawei2, set passwords to user1 and user2, set their phone numbers to 77730010 and 77730020 and use default values for other parameters.

   ```
   huawei(config-if-gpon-0/1)#sippstnuser add 0 1 1 mgid 1 username huawei1 telno
   77730010
   huawei(config-if-gpon-0/1)#sippstnuser add 0 2 1 mgid 1 username huawei2 telno
   77730020
   ```


Copyright © Huawei Technologies Co., Ltd.

Run the **display sippstnuser attribute** command to check whether the configuration of the POTS user is properly set.

```
huawei(config-if-gpon-0/1)#display sippstnuser attribute 0 1 1

---------------------------------------------------------------------------
  F/S/P                       : 0/1/0
  ONT ID                      : 1
  Port ID                     : 1

  MG ID                       : 1
  Telephone NO.               : 77730010
  User name                   : huawei1
  Password                    : user1
...//The rest of the response information is omitted.

huawei(config-if-gpon-0/1)#display sippstnuser attribute 0 2 1

---------------------------------------------------------------------------
  F/S/P                       : 0/1/0
  ONT ID                      : 2
  Port ID                     : 1

  MG ID                       : 1
  Telephone NO.               : 77730020
  User name                   : huawei2
  Password                    : user2
...//The rest of the response information is omitted.
```

Step 9 Apply and bind an ONT voice service profile to an SIP interface

Currently, the interface common profile, SIP agent profile, SIP service data profile, and POTS port profile can be applied to an SIP interface, and the digitmap profile can be bound to an SIP interface.

For profiles that can be applied to an SIP interface, if parameters in those profiles are changed, those profiles must be reapplied to the SIP interface so that the changed parameters can take effect. For profiles that can be bound to an SIP interface, if parameters in those profiles are changed, those profiles do not need to be rebound to the SIP interface and the changed parameters can take effect.

The method for applying an SIP agent profile is introduced in **Step 8.1**. The following will introduce the methods for applying an interface common profile, an SIP service data profile, and a POTS port profile, and the method for binding a digitmap to an SIP interface.

1. Apply an interface common profile.

   Run the **if-sip attribute** command to apply an interface common profile to an SIP interface or configure the interface customized parameters, or run the **ont-if-sip bat-apply from** command to bulk apply the interface common profiles to SIP interfaces. If you use these two commands to apply the interface common profiles or configure the interface customized parameters repeatedly, the last configurations take effect.

   In this example, the default interface common profile, namely interface common profile 1 is used.

2. Apply an SIP service data profile.

   Run the **sippstnuser rightflag** command to apply an SIP service data profile to an SIP interface or configure the interface customized parameters, or run the **ont-sippstnuser bat-apply from** command to bulk apply the SIP service data profiles to SIP interfaces. If you use these two commands to apply the SIP service data profiles or configure the interface customized parameters repeatedly, the last configurations take effect.

Copyright © Huawei Technologies Co., Ltd.

In this example, the default SIP service data profile, namely SIP service data profile 1 is used.

3. Apply a POTS port profile.

   Run the **pstnport electric** command to apply a POTS port profile to an SIP interface or configure the interface customized parameters, or run the **ont-pstnport electric bat-apply** command to bulk apply the POTS port profiles to SIP interfaces. If you use these two commands to apply the POTS port profiles or configure the interface customized parameters repeatedly, the last configurations take effect.

   In this example, the default POTS port profile, namely POTS port profile 1 is used.

4. Bind a digitmap profile.

   Run the **sippstnuser digitmap** command to bind a digitmap profile to an SIP interface, or run the **ont-sippstnuser bat-bind from** command to bulk apply the digitmap profiles to SIP interfaces. If you use these two commands to bind the SIP service data profiles to SIP ports repeatedly, the last configurations take effect.

   In this example, the default digitmap profile, namely digitmap profile 1 is used.

Step 10 (Optional) Configure the SIP user codec.

Run the **sippstnuser codec** command to configure the SIP user codec. The SIP user codec will not be configured independently in this example.

Step 11 Save the data.

```
huawei(config)#save
```

----End

9.7.3.9 Configuring the BTV Service

The OLT is connected to the remote gateway ONT through a GPON port to provide users with the bridge WAN multicast service.

Prerequisites

- The iTMS has configured the IPTV WAN ports on the ONT.
- The OLT has been connected to the BRAS and the multicast source.
- The VLAN of the LAN switch port connected to the OLT is the same as the upstream VLAN of the OLT.
- The ONT has been added to the OLT. For details, see **9.7.1.3 Adding an ONT to an OLT**.

Data Plan

Table 9-6 Data plan

Item	Data
ONT line profile	Profile name: ftth T-CONT ID: 4 GEM port ID: 13

Copyright © Huawei Technologies Co., Ltd.

Item	Data
Traffic profile	ID: 8 802.1p priority: 4 CIR: off (unlimited) Priority-based scheduling policy: local-setting
VLAN Plan	Single VLAN tag: ● SVLAN ID: 1000 ● MVLAN ID: 1000 ● VLAN type: smart ● VLAN attribute: common VLAN translation policy: ● ONT: duplicates multicast packets based on user ports and MVLANs are stripped off downstream. ● OLT: duplicates multicast packets based on PON ports with MVLAN unchanged.
Multicast service data	Multicast protocol: IGMP proxy Multicast version: IGMPv2 Multicast program: dynamic obtaining mode

Procedure

Step 1 Configure the OLT.

1. Configure a traffic profile.

   Configure traffic profile 8. Set the CIR to off (unlimited), priority to 4, and priority-based scheduling policy to local-setting (that is, queues are scheduled based on the priority specified in the profile).

   NOTE

   Run the **display traffic table ip** command to query the existing traffic profiles in the system. If the existing traffic profiles in the system do not meet the requirements, run the **traffic table ip** command to add a traffic profile.

   ```
   huawei(config)#traffic table ip index 8 cir off priority 4 priority-policy
   local-setting
   ```

2. Configure the mapping relationship between a GEM port and an Ethernet port on the ONT.

   If the ONT is connected to the STB through Ethernet port 2, map the service flow of Ethernet port 2 to GEM port 13 in the ONT line profile.

   ```
   huawei(config)#ont-lineprofile gpon profile-name ftth
   huawei(config-gpon-lineprofile-1)#mapping mode port
   huawei(config-gpon-lineprofile-1)#gem mapping 13 1 eth 2
   huawei(config-gpon-lineprofile-1)#commit
   huawei(config-gpon-lineprofile-1)#quit
   ```

3. Configure the multicast forwarding mode.

Copyright © Huawei Technologies Co., Ltd.

Configure the multicast forwarding mode is untagged.

```
huawei(config)#ont-srvprofile gpon profile-name ftth
huawei(config-gpon-srvprofile-1)#multicast-forward untag
huawei(config-gpon-srvprofile-1)#commit
huawei(config-gpon-srvprofile-1)#quit
```

4. Configure the VLAN of the Ethernet port on the ONT.

   If the ONT is connected to the STB through Ethernet port 2, add Ethernet port 2 to VLAN 1000.

```
huawei(config)#ont-srvprofile gpon profile-name ftth
huawei(config-gpon-srvprofile-1)#port vlan eth 2 1000
huawei(config-gpon-srvprofile-1)#multicast-forward untag
huawei(config-gpon-srvprofile-1)#commit
huawei(config-gpon-srvprofile-1)#quit
```

5. Create service flows.

   Set the service VLAN to 1000, GEM port ID to 13, and user VLAN to 1000, and use traffic profile 8.

```
huawei(config)#service-port 1 vlan 1000 gpon 0/1/0 ont 1 gemport 13 multi-
service
 user-vlan 1000 rx-cttr 8 tx-cttr 8
huawei(config)#service-port 2 vlan 1000 gpon 0/1/0 ont 2 gemport 13 multi-
service
 user-vlan 1000 rx-cttr 8 tx-cttr 8
```

6. Create an MVLAN and configure the IGMP version.

   Set the IGMP version for the MVLAN to IGMPv2.

```
huawei(config)#multicast-vlan 1000
huawei(config-mvlan1000)#igmp version v2
  This operation will delete all IPv4 programs with source IP addresses in the
current multicast VLAN
  Are you sure to change current IGMP version? (y/n)[n]:y
  Command is being executed. Please wait...
  Command has been executed successfully
```

7. Configure a program library.

   Set the mode for obtaining multicast programs to dynamic.

   NOTE

   You can set the mode for obtaining multicast programs to dynamic only when the IGMP mode is off.

```
huawei(config-mvlan1000)#igmp mode off
  Are you sure to close IGMP? (y/n)[n]:y
  Command is being executed. Please wait...
  Command has been executed successfully

huawei(config-mvlan1000)#igmp match mode disable
  Command has been executed successfully
```

   (Optional) Set the address range for the dynamic programs. If you need to limit the address range of dynamic programs, perform this operation. For example, set the address range of dynamic programs to 224.1.1.1-224.1.1.100.

```
huawei(config-mvlan1000)#igmp match group ip 224.1.1.1 to-ip 224.1.1.100
```

8. Set the IGMP mode.

   Select the IGMP proxy mode.

```
huawei(config-mvlan1000)#igmp mode proxy
  Are you sure to change IGMP mode? (y/n)[n]:y
```


Copyright © Huawei Technologies Co., Ltd.

```
  Command is being executed. Please wait...
  Command has been executed successfully
```

9. Configure the IGMP upstream port.

   Set the IGMP upstream port ID to 0/19/0 and working mode to **default**. Protocol packets are transmitted to all the IGMP upstream ports in the multicast VLAN.

```
huawei(config-mvlan1000)#igmp uplink-port 0/19/0
huawei(config-mvlan1000)#btv
huawei(config-btv)#igmp uplink-port-mode default
Are you sure to change the uplink port mode?(y/n)[n]:y
```

10. (Optional) Set multicast global parameters.

    In this example, the default settings are used for all the multicast global parameters.

11. Configure multicast users.

    Add service ports 1 and 2 as multicast users.

```
huawei(config-btv)#igmp user add service-port 1
huawei(config-btv)#igmp user add service-port 2
huawei(config-btv)#multicast-vlan 1000
huawei(config-mvlan1000)#igmp multicast-vlan member service-port 1
huawei(config-mvlan1000)#igmp multicast-vlan member service-port 2
huawei(config-mvlan1000)#quit
```

12. Save the data.

```
huawei(config)#save
```

Step 2 The ONT does not need to be configured.

----End

9.7.3.10 Configuring the VoD Service

The OLT is connected to the remote gateway ONT through a GPON port to provide users with the VoD service.

Prerequisites

- The iTMS has configured the IPTV WAN ports on the ONT.
- The OLT has been connected to the BRAS and the program source.
- The VLAN of the LAN switch port connected to the OLT is the same as the upstream VLAN of the OLT.
- The ONT has been added to the OLT. For details, see **9.7.1.3 Adding an ONT to an OLT**.

Data Plan

Item	Data
ONT line profile	Profile name: ftth T-CONT ID: 4 GEM port ID: 13

Copyright © Huawei Technologies Co., Ltd.

Item	Data
Traffic profile	ID: 8 802.1p priority: 4 CIR: off (unlimited) Priority-based scheduling policy: local-setting
VLAN Plan	Single VLAN tag: ● SVLAN ID: 1100 ● VLAN type: smart ● VLAN attribute: common ● CVLAN: 2001 VLAN translation policy: ● The ONT adds CVLAN tags (configured on the iTMS) to packets: untag<->C. ● The OLT implements VLAN translation: C<->S.

Procedure

Step 1 Configure the OLT.

1. Configure a traffic profile.

   Configure traffic profile 8. Set the CIR to off (unlimited), priority to 4, and priority-based scheduling policy to local-setting (that is, queues are scheduled based on the priority specified in the profile).

   NOTE

   Run the **display traffic table ip** command to query the existing traffic profiles in the system. If the existing traffic profiles in the system do not meet the requirements, run the **traffic table ip** command to add a traffic profile.

   ```
   huawei(config)#traffic table ip index 8 cir off priority 4 priority-policy
   local-setting
   ```

2. Configure the mapping relationship between a GEM port and a VLAN.

   The service flow of user VLAN 1100 is mapped to GEM port 13 in the ONT line profile.

   ```
   huawei(config)#ont-lineprofile gpon profile-name ftth
   huawei(config-gpon-lineprofile-1)#gem mapping 13 4 vlan 1100
   huawei(config-gpon-lineprofile-1)#commit
   huawei(config-gpon-lineprofile-1)#quit
   ```

3. Configure the VLAN of the Ethernet port on the ONT.

   If the ONT is connected to the STB through Ethernet port 2, add Ethernet port 2 to VLAN 1100.

   ```
   huawei(config)#ont-srvprofile gpon profile-name ftth
   huawei(config-gpon-srvprofile-1)#port vlan eth 2 1100
   huawei(config-gpon-srvprofile-1)#commit
   huawei(config-gpon-srvprofile-1)#quit
   ```

4. Create service flows.

Copyright © Huawei Technologies Co., Ltd.

Create service flows. Set the S-VLAN to 1100, GEM port ID to 13, and C-VLAN to 2001, and use traffic profile 8. Set the VLAN translation policy to Translate. The C-VLAN 2001 of the ONT is translated to S-VLAN 1100.

```
huawei(config)#service-port 3 vlan 1100 gpon 0/1/0 ont 1 gemport 13
multi-service user-vlan 2001 tag-transform translate rx-cttr 8 tx-cttr 8
huawei(config)#service-port 4 vlan 1100 gpon 0/1/0 ont 2 gemport 13
multi-service user-vlan 2001 tag-transform translate rx-cttr 8 tx-cttr 8
```

5. Save the data.

```
huawei(config)#save
```

Step 2 The ONT does not need to be configured.

----End

9.7.3.11 Configuring Link Aggregation, Congestion Control, and Security Policy

The global configuration of link aggregation and queue scheduling based on priorities ensures service reliability. The global configuration of security policies ensures service security.

Context

Link aggregation provides a higher bandwidth and uplink reliability for optical line terminals (OLTs) by aggregating multiple uplink Ethernet ports to one link aggregation group (LAG). Link aggregation is recommended.

Congestion control places the packets to be sent from a port into multiple queues that are marked with different priorities. Then, the packets are sent based on queue priorities. Congestion control is recommended.

Security policies ensure system, user, and service security.

NOTE

Enable a service security function based on the service type. For details, see **9.6.6 Principle of Security Data Plan**.

Procedure

- Configure link aggregation.

  The following configurations are used as an example to configure link aggregation:

  - Uplink ports 0/19/0 and 0/19/1 are added to a LAG.
  - The two ports send packets upstream based on the packets' source MAC addresses.
  - The LAG works in Link Aggregation Control Protocol (LACP) static aggregation mode.

  ```
  huawei(config)#link-aggregation 0/19 0-1 ingress workmode lacp-static
  ```

- Configure queue scheduling.

  According to quality of service (QoS) planning principles, all packets are scheduled in strict priority (SP) mode and mapped to queues according to the packets' priorities. For details about QoS planning principles, see **11.2.2 Principle of QoS Data Plan**.

  ```
  huawei(config)#queue-scheduler strict-priority
  huawei(config)#cos-queue-map cos0 0 cos4 4 cos5 5 cos6 6
  ```

- Configure system security.
  - Enable deny of service (DoS) anti-attack on the OLT.

Copyright © Huawei Technologies Co., Ltd.

1. Run the **security anti-dos enable** command to globally enable DoS anti-attack.
2. Run the **security anti-dos control-packet policy** command to configure a protocol packet processing policy that will be used when a DoS attack occurs.
3. Run the **security anti-dos control-packet rate** command to configure the threshold for the rate of sending protocol packets to the CPU.

- Enable IP address anti-attack on the OLT.

  Run the **security anti-ipattack enable** command to enable IP address anti-attack.

- Configure user security.
  - Enable MAC address anti-flapping on the OLT.

    Run the **security anti-macduplicate enable** command to enable MAC address anti-flapping.
  - Enable MAC address anti-spoofing on the OLT.
    1. In global config mode, run the **security anti-macspoofing enable** command to globally enable MAC address anti-spoofing.
    2. Enable MAC address anti-spoofing at VLAN level in global config mode or service profile mode:
       a. In global config mode, run the **security anti-macspoofing vlan** command to enable MAC address anti-spoofing.
       b. In global config mode, run the **vlan service-profile** command to create a VLAN service profile.
       c. Perform the following operations to enable MAC address anti-spoofing in VLAN service profile mode:
          a. Run the **security anti-macspoofing enable** command to enable MAC address anti-spoofing at VLAN level.
          b. Run the **commit** command to make the profile configuration take effect.
          c. Run the **quit** command to quit the VLAN service profile mode.
          d. Run the **vlan bind service-profile** command to bind the created VLAN service profile to a VLAN.
    3. (Optional) Run the **security anti-macspoofing max-mac-count** command to set the maximum number of MAC addresses that can be bound to a service flow.
    4. (Optional) Run the **security anti-macspoofing exclude** command to configure the types of packets for which MAC address anti-spoofing does not take effect, such as Internet Group Management Protocol (IGMP) packets.
  - Enable IP address anti-spoofing on the OLT.

    IP address anti-spoofing can be enabled or disabled at three levels: global, VLAN, and service port levels. This function takes effect only after it is enabled at the three levels. Among the three levels, IP address anti-spoofing is disabled only at the global level by default.
    1. In global config mode, run the **security anti-ipspoofing enable** command to enable IP address anti-spoofing at the global level.
    2. In VLAN service profile mode, run the **security anti-ipspoofing enable** command to enable IP address anti-spoofing at the VLAN level.

Copyright © Huawei Technologies Co., Ltd.

3. Run the **security anti-ipspoofing service-port** *serviceport-id* **enable** command to enable IP address anti-spoofing at the service port level.

- Configure service security.
  - Enable Dynamic Host Configuration Protocol (DHCP) Option 82 on the OLT. This configuration is recommended for the DHCP-based Internet access service.
    1. Enable DHCP Option 82 on the OLT.

       DHCP Option 82 can be enabled or disabled at four levels: global, port, VLAN, and service port levels. This function takes effect only after it is enabled at the four levels. Among the four levels, DHCP Option 82 is disabled only at the global level by default.

       - The global level: In global config mode, run the **dhcp option82** command to enable DHCP Option 82 at the global level.

         When you run this command, select the **enable**, **forward**, or **rebuild** parameter based on site requirements. The three parameters can all enable DHCP Option 82 but provide different packet processing policies on the OLT. For details, see the **dhcp option82** command.
       - The port level: In global config mode, run the **dhcp option82 port** or **dhcp option82 board** command to enable DHCP Option 82 at the port level.
       - The VLAN level:
         a. In global config mode, run the **vlan service-profile** command to create a VLAN service profile.
         b. Run the **dhcp option82 enable** command to enable DHCP Option 82 at the VLAN level.
         c. Run the **commit** command to make the profile configuration take effect.
         d. Run the **quit** command to quit the VLAN service profile mode.
         e. Run the **vlan bind service-profile** command to bind the created VLAN service profile to a VLAN.
       - The service port level: In global config mode, run the **dhcp option82 service-port** command to enable DHCP Option 82 at the service port level.
    2. On the OLT, run the **dhcp-option82 permit-forwarding service-port** command with the **enable** parameter selected, to allow ONT DHCP packets to carry Option 82 information.
  - Enable Policy Information Transfer Protocol (PITP) on the OLT. This configuration is recommended for the PPPoE-based Internet access service.
    1. Enable PITP on the OLT.

       PITP can be enabled or disabled at four levels: global, port, VLAN, and service port levels. This function takes effect only after it is enabled at the four levels. Among the four levels, PITP is disabled only at the global level by default.

       - The global level: In global config mode, run the **pitp enable pmode**, **pitp forward pmode**, or **pitp rebuild pmode** command to enable PITP at the global level.

         In the preceding commands, the **enable**, **forward**, and **rebuild** parameters can all enable PITP but provide different packet processing policies on the

Copyright © Huawei Technologies Co., Ltd.

OLT. Select one of them based on site requirements. For details, see the **pitp** command.

- The port level: In global config mode, run the **pitp port** or **pitp board** command to enable PITP at the port level.
- The VLAN level:
  a. In global config mode, run the **vlan service-profile** command to create a VLAN service profile.
  b. Run the **pitp enable** command to enable PITP at the VLAN level.
  c. Run the **commit** command to make the profile configuration take effect.
  d. Run the **quit** command to quit the VLAN service profile mode.
  e. Run the **vlan bind service-profile** command to bind the created VLAN service profile to a VLAN.
- The service port level: In global config mode, run the **pitp service-port** command to enable PITP at the service port level.

2. On the OLT, run the **pitp permit-forwarding service-port** command with the **enable** parameter selected, to allow ONT PPPoE packets to carry a vendor tag.

----End

9.7.3.12 Verifying Services

In the FTTH scenario, ONTs are installed in users' houses which are far away from the central equipment room. ONTs provide remote service verification methods including PPPoE dialup emulation, call emulation, and multicast emulation to facilitate configuration and commissioning engineers to verify services remotely after service configuration.

Prerequisites

ONTs and upper-layer devices have been connected properly. The BRAS and MGC/IMS have been configured.

Background

Remote Service Verification Method	Function	Description
PPPoE dialup emulation	An ONT simulates a PPPoE user terminal software to perform dialup and interact with the BRAS to verify the connectivity between the ONT and BRAS.	● PPPoE dialup emulation requires a service flow which does not belong to a QinQ VLAN. ● A user name, password, and authentication mode must be configured on the BRAS for the PPPoE dialup emulation. ● An ONT supports a maximum of a PPPoE dialup emulation.

Copyright © Huawei Technologies Co., Ltd.

Remote Service Verification Method	Function	Description
Call Emulation	An ONT simulates a voice user to make a call to check whether the voice service data is correctly configured. You can also use the call emulation function to locate a fault when the voice service is faulty.	● An ONT can simulate a caller or callee to communicate with a phone in a call. In this case, only a functional phone is required in the central office where the acceptance personnel is. ● An ONT supports a maximum of a call emulation.
Multicast emulation	This function enables you to simulate a multicast user going online and lead the program stream to an ONT. You can check whether the multicast service is normal by checking the real-time traffic of the multicast program.	Multicast services configured in the dynamic controllable multicast mode do not support this function.

Data plan

Item	Data	Remarks
PPPoE dialup emulation parameters	PPPoE user name: test@huawei Password: test	The user name, password, and authentication mode for the emulation test must be configured on the BRAS. The entered user name, password, and authentication mode must be consistent with those configured on the BRAS.
Call emulation parameters	ONT POTS ID: 1	The default values are used. You can run the **display pots emulational configuration** command to check the parameter values.
Multicast emulation parameters	Multicast service flow ID: 1 MVLAN: 1000 IP address of the multicast program: 224.1.1.10	-

Procedure

- Verify the Internet access service using PPPoE dialup emulation.
  1. In the xPON board mode, run the **pppoe simulate start** command to start a PPPoE dialup emulation test. The following test uses GPON as an example:

Copyright © Huawei Technologies Co., Ltd.

```
huawei(config)#interface gpon 0/1
huawei(config-if-gpon-0/1)#pppoe simulate start
{ portid<U><0,7> }:0
{ ontid<U><0,127> }:1
{ eth<K>|untagged<K>|vlanid<U><0,4095> }:eth
{ ont-portid<U><1,8> }:4
{ untagged<K>|vlanid<U><0,4095> }:100
{ priority<U><0,7>|user-name<K> }:user-name
{ username<S><Length 1-64> }:test@huawei
{ user-password<K> }:user-password
{ password<S><Length 1-64> }:test
{ authentication-mode<K> }:authentication-mode
{ protocol<E><chap,pap> }:chap

  Command:
          pppoe simulate start 0 1 eth 4 100 user-name test@huawei user-
password
 test authentication-mode chap

huawei(config-if-gpon-0/1)#
  ---------------------------------
  ONT PPPoE Test Result
  ---------------------------------
  F/S/P                : 0/1/0
  ONT-ID               : 1
  ONT ETH Port ID      : 4
  ONT Vlan ID          : 100
  Vlan Priority        : -
  Emluator result      : Success
  Session ID           : 18814
  User IP              : 192.168.100.101
  Gateway IP           : 192.168.100.1
  ---------------------------------
```

- Troubleshooting methods for the Internet access service
  1. Check whether configurations are complete on the OLT.
     - Run the **display ont info** command to query the ONT status to check whether the ONT is registered successfully.
     - Run the **display service-port** command to check whether the Internet access service flow is configured and whether the inner VLAN ID of the service flow is consistent with that in the data plan.
     - If a native VLAN is configured for the Ethernet port on the ONT, run the **display ont port attribute** command in the xPON board mode to check whether the native VLAN is correct.
  2. Check the upstream and downstream ports by checking the MAC address learning status.
     a. Run the **display mac-address vlan** command to check the MAC address learning status of the Internet service VLAN.
        - If the upstream port does not learn a MAC address, check the network connections between the upstream port and upper-layer devices and check the configurations of upper-layer devices.
        - If the downstream port does not learn a MAC address, check whether the ONT is activated, whether the PC is connected to the right port on the ONT, and whether the PC is working properly.
     b. Run the **display ont-learned-mac** command to check whether the ONT connecting to the PON port learned any MAC addresses.

Copyright © Huawei Technologies Co., Ltd.

If not, check whether the ONT properly connects to the PC or home gateway (HGW).

- Verify the voice service using call emulation.
  1. Run the **ont emulational call** command to configure a call emulation test.

```
huawei(config)#test
huawei(config-test)#ont emulational call caller-port 0/1/0 1 1 telno
77730020
{ <cr>|caller-stop-time<K> }:

  Command:
          ont emulational call caller-port 0/1/0 1 1 telno 77730020
```

  2. The ONT outputs the call emulation result after the test is complete.

```
huawei(config-test)#
  ------------------------------------------------------------------
  F/S/P                : 0/1/0
  ONT-ID               : 0
  ONT-POTSID           : 1
  Test type            : caller emulational call test
  Detected number      : 77730020
  Reported number      : 77730020
  Current status       : test end
  Test Result          : success
  ------------------------------------------------------------------
```

- Troubleshooting methods for the voice service.
  1. Check whether configurations are complete on the OLT.
     - Run the **display ont info** command to query the ONT status to check whether the ONT is registered successfully.
     - Run the **display service-port** command to check whether the voice service flow is configured and whether the inner VLAN ID of the service flow is consistent with that in the data plan.
  2. Check the upstream and downstream ports by checking the MAC address learning status.

     Run the **display mac-address vlan** command to check the MAC address learning status of the voice service VLAN.
     - If the upstream port does not learn a MAC address, check the network connections between the upstream port and upper-layer devices and check the configurations of upper-layer devices.
     - If the downstream port does not learn a MAC address, check whether the ONT is activated and whether physical links are normal.
     - If both the upstream and downstream ports can learn the MAC address, record the MAC address of the ONT and log in to the service router (SR) to check whether an IP address is allocated to the MAC address.
  3. Check the registration status of the voice service.
     - You can run the **display ont port state** command on the OLT to query the call connection status on the POTS port. If **Call State** is **RegisterFail** or **Connecting** for a long time, check whether the voice configuration on the MGC/SIP server is consistent with that on the ONT.
     - If the ONT uses the H.248 protocol, you can run the **display ont mg status** command on the OLT to query the registration status of the MG interface that connects to the ONT. If **MG Status** is **UnRegistered** or **Registering** for a long

Copyright © Huawei Technologies Co., Ltd.

time, check whether the voice configuration on the MGC/SIP server is consistent with that on the ONT.

- You can query the registration status of the voice service on the ONT web page. If the query result shows that the registration fails or the voice service is in the registering state for a long time, check whether the voice configuration on the MGC/SIP server is consistent with that on the ONT.

- Verify the multicast service using multicast emulation.

  1. Run the **igmp static-join** command to simulate a multicast user to order a multicast program.

     ```
     huawei(config)#btv
     huawei(config-btv)#igmp static-join service-port 1 ip 224.1.1.10 vlan 1000
     ```

     NOTE

     If the multicast program is obtained dynamically, **igmp static-join** can be executed successfully only when the range for obtaining the dynamic program is set.

  2. Run the **display igmp user** command to query the status of the multicast user.

     ```
     huawei(config-btv)#display igmp user service-port 1
       User                        : 0/1/0/1
       State                       : online
       Authentication              : no-auth
       Quick leave                 : MAC-based
       IGMP flow ID                : 1
       Video flow ID               : 1
       Log switch                  : enable
       Bind profiles               : -
       IGMP version                : IGMP v3
       Current version             : IGMP v3
       Current IGMP IPv6 version   : IGMP IPv6 v2
       Available programs          : 8
       Global leave                : disable
       User max bandwidth          : no-limit
       Used bandwidth(kbps)        : 0
       Used bandwidth
       to max bandwidth(%)         : -
       Total video bandwidth       : -
       Mcast video bandwidth       : -
       Active program list

     ------------------------------------------------------------------------
     --
       Program name     VLAN  IP/MAC           State           Start time

     ------------------------------------------------------------------------
     --
       PROGRAM-5        1000  224.1.1.10       watching        2011-10-29
                                                               16:33:41+08:00

     ------------------------------------------------------------------------
     --
       Total: 1
     ```

  3. Run the **display multicast flow-statistic** command to query the real-time traffic of the multicast program.

     ```
     huawei(config-btv)#display multicast flow-statistic vlan 1000 ip
     224.1.1.10
     { <cr>|sourceip<K> }:

       Command:
               display multicast flow-statistic vlan 1000 ip 224.1.1.10
     ```


Copyright © Huawei Technologies Co., Ltd.

```
Command is being executed. Please wait...
Multicast flow statistic result: 8736(kbps)
```

----End

9.7.4 Configuring Triple Play Service (Simplified Mode)

The GPON service configuration in simplified mode is implemented by creating an end-to-end (E2E) service port between an OLT and an ONT. This topic describes how to achieve the GPON service configuration in simplified mode by configuring the Internet access service, voice service, and multicast service in the FTTH scenario.

Service Requirements

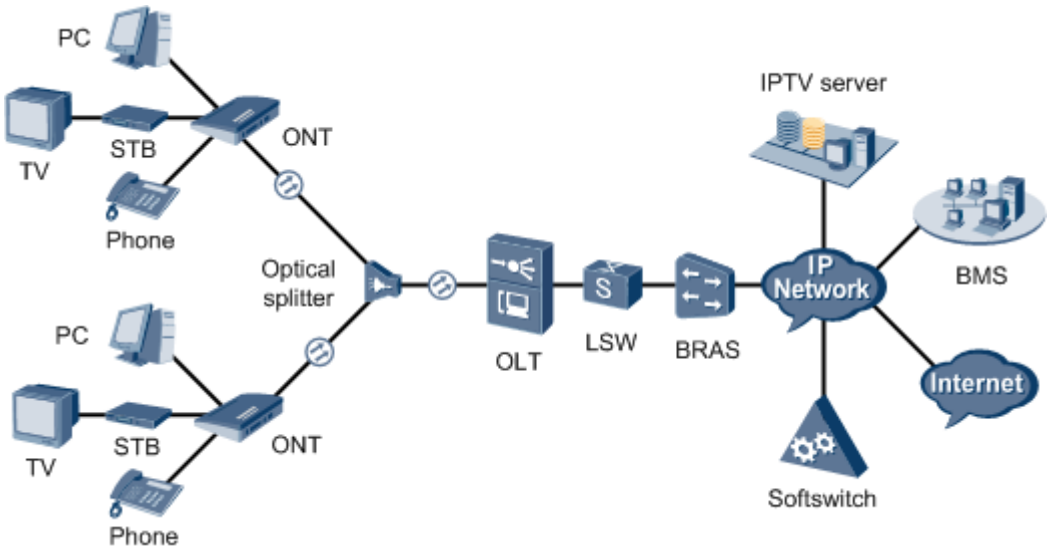
NOTE

On the same ONT, service ports in the simplified mode conflict with services ports in the profile mode. Therefore, they cannot be configured concurrently.

- Subscribers use the bridging ONTs (supporting VoIP). The PC, STB, and phone are connected to different ports on the ONT to achieve the triple play service.
- Different services are distinguished by different S-VLANs on an OLT.
- The internet access service has a rate restriction of 4 Mbit/s both in upstream and downstream directions.
- IPTV service has no rate restriction in upstream or downstream direction.
- The VoIP adopts the H.248 protocol and the phones connected to different ONTs can communicate with each other.

Figure 9-7 shows an example network of the FTTH triple play service.

Figure 9-7 Example network of the FTTH triple play service



Prerequisite

- The OLT is connected to the BRAS, MGC, and the multicast source.

Copyright © Huawei Technologies Co., Ltd.

- The interface data and the POTS user configuration data corresponding to the MG interface is configured on the MGC.
- Related configurations are performed on the BRAS according to the authentication and accounting requirements for dialup users. For details about the configuration, see the configuration guide.
- The VLAN of the LAN switch port connected to the OLT is consistent with the upstream VLAN of the OLT.

Procedure

- Configure the OLT.
  1. Configure GPON ONT profiles.

     GPON ONT profiles include the DBA profile, line profile, service profile, and alarm profile. In the simplified mode, the default DBA profile, line profile, and service profile are used. That is, these profiles do not need to be configured.

     a. Add an ONT line profile

        The default line profile 0 is used. In this profile, the default T-CONT 0 and T-CONT 1 are created. T-CONT 0 is bound to the default DBA profile 2 (the fixed bandwidth: 1 Mbit/s), and is used for the OMCI management channel. T-CONT 1 is bound to the default DBA profile 0 (the assured bandwidth: 8 Mbit/s, the maximum bandwidth: 20 Mbit/s), and is used for the service channel. The DBA profile bound to a T-CONT can be modified.

     b. Add an ONT service profile

        The default service profile 0 is used. In this profile, the capability set of the ETH port and POTS port is set to **adaptive** by default and therefore the OLT automatically matches the number of ports according to the type of the online ONT.

     c. (Optional) Add an alarm profile.

        - The default GPON alarm profile 1 is used. The alarm thresholds of the default alarm profile are 0, which indicates that no alarm is generated.
        - In this example, the default alarm profile is used, and therefore the configuration of the alarm profile is not required.
        - Run the **gpon alarm-profile add** command to configure a GPON alarm profile, which is used for monitoring the performance of an activated ONT line.

  2. Add ONTs on the OLT.

     The ONT is connected to a GPON port of the OLT by optical fibers. The service can be configured only after ONTs are successfully added on the OLT.

     Two ONTs are connected to GPON port 0/1/1. The ONT IDs are 1 and 2, SNs are 32303131D659FD40 and 6877687714852901, passwords are 0100000001 and 0100000002, the discovery mode of passwords is once-on, and the management mode is OMCI.

     a. Add ONTs offline.

        If the password of an ONT is known, run the **ont add** command to add an ONT offline.

Copyright © Huawei Technologies Co., Ltd.

```
huawei(config)#interface gpon 0/1
huawei(config-if-gpon-0/1)#ont add 1 1 password-auth 0100000001 once-
on no-aging omci
huawei(config-if-gpon-0/1)#ont add 1 2 password-auth 0100000002 once-
on no-aging omci
```

b. Discover ONTs automatically.

If the password or SN of an ONT is unknown, run the **port *portid* ont-auto-find** command in GPON mode to enable the ONT auto-discovery function of the GPON port. Then, run the **ont confirm** command to confirm the ONT.

```
huawei(config)#interface gpon 0/1
huawei(config-if-gpon-0/1)#port 1 ont-auto-find enable
huawei(config-if-gpon-0/1)#display ont autofind 1
   //After this command is executed, the information of all ONTs
connected to the GPON port through optical splitters is displayed.

------------------------------------------------------------------------
---
   Number              : 1
   F/S/P               : 0/1/1
   Ont SN              : 32303131D659FD40
   Password            :
   VenderID            : HWTC
   Ont Version         : 120A0000
   Ont SoftwareVersion : V1R001C01
   Ont EquipmentID     : EchoLife:HG8245
   Ont autofind time   : 2009-10-24 14:59:10

------------------------------------------------------------------------
---
   Number              : 2
   F/S/P               : 0/1/1
   Ont SN              : 6877687714852901
   Password            :
   VenderID            : HWTC
   Ont Version         : 120A0000
   Ont SoftwareVersion : V1R001C01
   Ont EquipmentID     : EchoLife:HG8245
   Ont autofind time   : 2009-10-24 14:59:12

------------------------------------------------------------------------
---
huawei(config-if-gpon-0/1)#ont confirm 1 ontid 1 sn-auth
32303131D659FD40 omci
huawei(config-if-gpon-0/1)#ont confirm 1 ontid 2 sn-auth
6877687714852901 omci
```

c. (Optional) Bind the alarm profile to the ONT.

The default profile 1 is used in this example.

```
huawei(config-if-gpon-0/1)#ont alarm-profile 1 1 profile-id 1
huawei(config-if-gpon-0/1)#ont alarm-profile 1 2 profile-id 1
```

3. Confirm that the ONTs go online successfully.

After an ONT is added, run the **display ont info** command to query the current status of the ONT. Ensure that **Config flag** of the ONT is **active**, **Run State** is **online**, **Config state** is **normal**, and **Match state** is **match**.

```
huawei(config-if-gpon-0/1)#display ont info 1 1

------------------------------------------------------------------------

  F/S/P               :
0/1/1
  ONT-ID              :
```


Copyright © Huawei Technologies Co., Ltd.

```
1
  Control flag         : active    //Indicates that the ONT is
activated.
  Run state            : online    //Indicates that the ONT goes online
successfully.
  Config state        : normal    //Indicates that the configuration state
of the ONT is normal.
  Match state          : match     //Indicates that the capability profile
bound to the ONT is consistent with the actual capability of the ONT.
...//The rest of the response information is omitted.
```

When **Config state** is **failed**, **Run state** is **offline**, or **Match state** is **mismatch**:

- If **Control flag** is **deactive**, run the **ont active** command in GPON mode to activate the ONU.
- If **Run state** is **offline**, a physical line may be disconnected or the optical module may be damaged. Check the line and the optical module.
- If **Config state** is **failed**, the configured ONU capability exceeds the actual ONU capability. In this case, run the **display ont failed-configuration** command in the diagnose mode to check the failed configuration item and the failure cause. Then, rectify the fault accordingly.

  NOTE

  If the ONT only supports 4 queues, the priority-queue parameter of the **gem add** command is invalid when the priority-queue value is set to 4-7. Consequently **Config state** is **failed**.

- If the ONU does not match, that is, **Match state** is **mismatch**, the port types and number of ports undermatch the actual port types and number of ports supported by the ONU. In this case, run the **display ont capability** command to query the actual capability of the ONU, and then select one of the following modes to modify the ONU configuration:
  - Create a proper ONU profile according to the actual capability of the ONU, and then run the **ont modify** command to modify the configuration data of the ONU.
  - Modify the ONU profile according to the actual capability of the ONU and save the modification. Then, the ONU automatically recovers the configuration successfully.

4. Configure the Internet access service.

   a. Create an S-VLAN and add an upstream port to it.

      The VlAN ID is 100, and the VLAN type is smart. Add upstream port 0/19/0 to smart VLAN 100.

      ```
      huawei(config)#vlan 100 smart
      huawei(config)#port vlan 100 0/19 0
      ```

   b. Configure a traffic profile.

      Run the **display traffic table ip** command to query existing traffic profiles in the system. If the traffic profiles existing in the system do not meet the requirements, you need to run the **traffic table ip** command to add a traffic profile.

      Set the profile ID to 8, the CIR to 4 Mbit/s, and the priority to 1. In addition, configure the scheduling mode so that packets are scheduled according to their priorities.

Copyright © Huawei Technologies Co., Ltd.

```
huawei(config)#traffic table ip index 8 cir 4096 priority 1 priority-
policy
 local-setting
```

c. Create a service port.

Set the service port indexes to 1 and 2, S-VLAN ID to 100, and C-VLAN ID to 10. The user PC is connected to EHT port 1 on the ONT. The traffic profile 8 is used.

NOTICE

The user PC is connected to the ONT port. Therefore, the user-side VLAN is set to untagged.

```
huawei(config)#service-port 1 vlan 100 port 0/1/1 ont 1 eth 1 multi-
service
 user-vlan untagged inbound traffic-table index 8 outbound traffic-
table index 8
huawei(config)#service-port 2 vlan 100 port 0/1/1 ont 2 eth 1 multi-
service
 user-vlan untagged inbound traffic-table index 8 outbound traffic-
table index 8
```

5. Configure the voice service.

a. Create an S-VLAN and add an upstream port to it.

The VlAN ID is 200, and the VLAN type is smart. Add upstream port 0/19/0 to smart VLAN 200.

```
huawei(config)#vlan 200 smart
huawei(config)#port vlan 200 0/19 0
```

b. Enable ARP proxy.

For different users of the same S-VLAN, because the service ports of the smart VLAN are isolated from each other, the voice media streams cannot interchange normally. The ARP proxy function of the OLT must be enabled so that different users of the same VLAN can communicate with each other.

```
huawei(config)#arp proxy enable
huawei(config)#interface vlanif 200
huawei(config-if-vlanif200)#arp proxy enable
huawei(config-if-vlanif200)#quit
```

c. Configure a traffic profile.

Run the **display traffic table ip** command to query existing traffic profiles in the system. If the traffic profiles existing in the system do not meet the requirements, you need to run the **traffic table ip** command to add a traffic profile.

Set the profile ID to 9, the priority to 6 and no rate limitation on both the upstream and downstream directions. In addition, configure the scheduling mode so that packets are scheduled according to their priorities.

```
huawei(config)#traffic table ip index 9 cir off priority 6 priority-
policy
 local-setting
```

d. Create a service port.

Copyright © Huawei Technologies Co., Ltd.

Set the service port indexes to 3 and 4, S-VLAN ID to 200, and C-VLAN ID to 20. The user phone is connected to the POTS port on the ONT. The traffic profile 9 is used.

```
huawei(config)#service-port 3 vlan 200 port 0/1/1 ont 1 iphost multi-service
 user-vlan 20 inbound traffic-table index 9 outbound traffic-table index 9
huawei(config)#service-port 4 vlan 200 port 0/1/1 ont 2 iphost multi-service
 user-vlan 20 inbound traffic-table index 9 outbound traffic-table index 9
```

6. Configure the multicast service.

   a. Create an S-VLAN and add an upstream port to it.

      The VlAN ID is 1000, and the VLAN type is smart. Add upstream port 0/19/0 to smart VLAN 1000.

      ```
      huawei(config)#vlan 1000 smart
      huawei(config)#port vlan 1000 0/19 0
      ```

   b. Configure a traffic profile.

      Run the **display traffic table ip** command to query existing traffic profiles in the system. If the traffic profiles existing in the system do not meet the requirements, you need to run the **traffic table ip** command to add a traffic profile.

      Set the profile ID to 10, the priority to 4 and no rate limitation on both the upstream and downstream directions. In addition, configure the scheduling mode so that packets are scheduled according to their priorities.

      ```
      huawei(config)#traffic table ip index 10 cir off priority 4 priority-policy
       local-setting
      ```

   c. Create a service port.

      Set the service port indexes to 5 and 6, S-VLAN ID to 1000, C-VLAN ID to 30, and the ID of the ONT ETH port connected to the user STB to 2. The traffic profile 10 is used.

      NOTE

      If the STB interconnected to the ONT does not support VLAN tag, the user-side VLAN is set to untagged when creating service port.

      ```
      huawei(config)#service-port 5 vlan 1000 port 0/1/1 ont 1 eth 2 multi-service
       user-vlan 30 inbound traffic-table index 10 outbound traffic-table index 10
      huawei(config)#service-port 6 vlan 1000 port 0/1/1 ont 2 eth 2 multi-service
       user-vlan 30 inbound traffic-table index 10 outbound traffic-table index 10
      ```

   d. Configure the IGMP version.

      Set the IGMP version of the multicast VLAN to IGMPv3.

      ```
      huawei(config)#multicast-vlan 1000
      huawei(config-mvlan1000)#igmp version v3
      ```

   e. Create a multicast VLAN and select the IGMP mode.

      Set the multicast VLAN ID to 1000 and select the IGMP proxy mode.

      ```
      huawei(config-mvlan1000)#igmp mode proxy
        Are you sure to change IGMP mode?(y/n)[n]:y
      ```


Copyright © Huawei Technologies Co., Ltd.

f. Configure an IGMP upstream port.

Set the IGMP upstream port to port 0/19/0 and working mode to **default**. Protocol packets are transmitted to all the IGMP upstream ports in the multicast VLAN.

```
huawei(config-mvlan1000)#igmp uplink-port 0/19/0
huawei(config-mvlan1000)#btv
huawei(config-btv)#igmp uplink-port-mode default
Are you sure to change the uplink port mode?(y/n)[n]:y
```

g. (Optional) Set the multicast global parameters.

In this example, the default settings are used for all the multicast global parameters.

h. Configure a program library.

Configure the IP address of the multicast program to 224.1.1.10, program name to program1, and program source IP address to 10.10.10.10.

```
huawei(config-btv)#multicast-vlan 1000
huawei(config-mvlan1000)#igmp program add name program1 ip 224.1.1.10
sourceip
 10.10.10.10
```

i. Configure a right profile.

Configure a profile named profile0, with the right of watching program 1.

```
huawei(config-mvlan1000)#btv
huawei(config-btv)#igmp profile add profile-name profile0
huawei(config-btv)#igmp profile profile-name profile0 program-name
program1 watch
```

j. Configure multicast users.

Configure users of service ports 5 and 6 as multicast users and bind right profile profile0 to the service ports.

```
huawei(config-btv)#igmp user add service-port 5 auth
huawei(config-btv)#igmp user add service-port 6 auth
huawei(config-btv)#igmp user bind-profile service-port 5 profile-name
profile0
huawei(config-btv)#igmp user bind-profile service-port 6 profile-name
profile0
huawei(config-btv)#multicast-vlan 1000
huawei(config-mvlan1000)#igmp multicast-vlan member service-port 5
huawei(config-mvlan1000)#igmp multicast-vlan member service-port 6
huawei(config-mvlan1000)#quit
```

7. Save the data.

```
huawei(config)#save
```

- Configure the ONT.

  The ONT does not need to be configured for the Internet access service and multicast service. For the voice service, configurations on the ONT are consistent with those in the profile mode.

----End

Result

- Use the PPPoE dialup software to dial on the PC. After the dialup is successful, the user can access the Internet.
- Connect two phones to two TEL ports of different ONTs, and subscribers can use these two phones to call each other.

Copyright © Huawei Technologies Co., Ltd.

- The subscriber can watch program 1 on the TV.

9.8 P2P Access: Configuring FTTH Service

Users connected to the OLT through an ONT, and are therefore provided with the Internet, VoIP, and IPTV service through a same port.

Service Requirements

- ONT_1 and ONT_2 are provided with the triple play service through FTTH.
- The Internet access service is provided in the PPPoE access mode.
- The IPTV user connected to ONT_1 can watch all the programs, and the IPTV user connected to ONT_2 can watch only program BTV-1.
- The VoIP service and the IPTV service are provided in the DHCP mode and obtain IP addresses from the DHCP server in the DHCP option-60 mode.
- After receiving different traffic streams, the OLT provides different QoS guarantees to the traffic streams according to the priorities of the traffic streams.
- Traffic streams are differentiated on the OLT by the user-side VLAN (C-VLAN).

Figure 9-8 Example network of the optical fiber access service in the single-port for multiple services mode

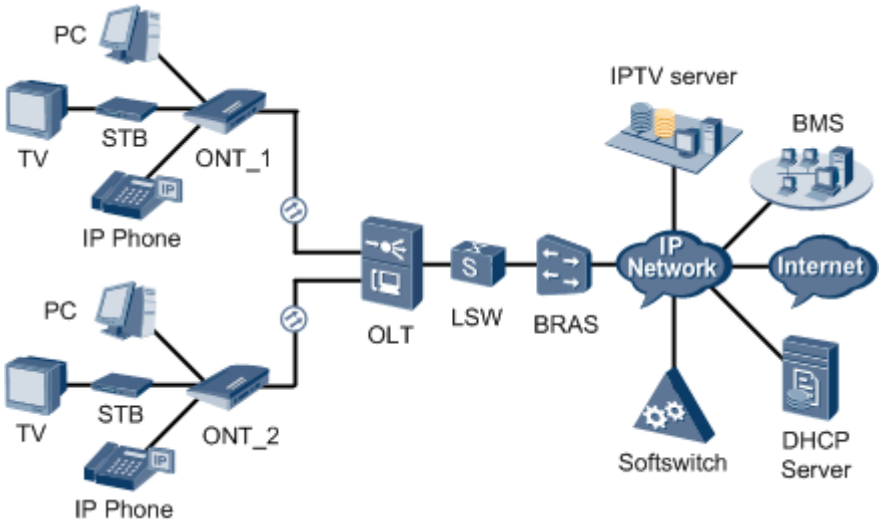


Table 9-7 Data plan for configuring the VLANs

Configuration Item	Data Item	Data
SVLAN	HSI service	SVLAN: 100 CVLAN: 2
	IPTV service	SVLAN: 1000 CVLAN: 4

Copyright © Huawei Technologies Co., Ltd.

Configuration Item	Data Item	Data
	VoIP service	SVLAN: 200 CVLAN: 3
IPTV service data	Multicast protocol	IGMP proxy
	Multicast version	IGMP V3
	Configuration mode of the multicast program	Static configuration mode
	IP address of the multicast server	10.10.10.10
	Multicast DHCP server group	20.2.2.2 20.2.2.3
	Multicast program	BTV-1: 224.1.1.10 BTV-2: 224.1.1.20
QoS (priority)	HSI service	Priority: 1; queue scheduling: WRR
	IPTV service	Priority: 4; queue scheduling: WRR
	VoIP service	Priority: 5; queue scheduling: PQ
VoIP service data	VoIP DHCP server group	20.1.1.2 20.1.1.3

Prerequisite

- The OLT is connected to the upper-layer devices such as the BRAS, multicast server, SoftX3000, and DHCP server.
- The VLAN of the LAN switch port connected to the OLT is the same as the upstream VLAN of the OLT.
- The OLT uses the OPFA board or the OPGD board to connect to the ONT.

Procedure

- Configure the Internet access service on the OLT.
  1. Create a VLAN and add an upstream port to the VLAN.

     The VLAN ID is 100, and the VLAN is a smart VLAN. The upstream port is 0/19/0.

     ```
     huawei(config)#vlan 100 smart
     huawei(config)#port vlan 100 0/19 0
     ```

  2. Configure a traffic profile.

     Because the VoIP, IPTV, and Internet access services are provided through the same port, you must set the 802.1p priority of each service. Generally, the priorities are in

Copyright © Huawei Technologies Co., Ltd.

a descending order for the VoIP service, IPTV service, and Internet access service. In this example, set the traffic profile index to 7 and the priority of the Internet access service to 1.

```
huawei(config)#traffic table ip index 7 cir 10240 priority 1 priority-
policy
 local-Setting
```

3. Configure a service port.

   Add a service port to the VLAN and use traffic profile 7. The user-side VLAN ID is 2.

```
huawei(config)#service-port vlan 100 eth 0/5/2 multi-service user-vlan 2
 rx-cttr 7 tx-cttr 7
huawei(config)#service-port vlan 100 eth 0/5/3 multi-service user-vlan 2
rx-cttr
 7 tx-cttr 7
```

4. Configure queue scheduling.

   Use the 3PQ+5WRR queue scheduling. Queues 0-4 adopt the WRR mode, with the weights of 10, 10, 20, 20, and 40 respectively; queues 5-7 adopt the PQ mode.

   NOTE

   Queue scheduling is a global configuration. You need to configure queue scheduling only once on the OLT, and then the configuration takes effect globally. In the subsequent phases, you need not configure queue scheduling repeatedly when configuring other services.

```
huawei(config)#queue-scheduler wrr 10 10 20 20 40 0 0 0
```

   Configure the mapping between queues and 802.1p priorities. Priorities 0-7 map queues 0-7 respectively.

```
huawei(config)#cos-queue-map cos0 0 cos1 1 cos2 2 cos3 3 cos4 4 cos5 5 cos6
6
 cos7 7
```

   NOTE

   For the service board that supports only four queues, the mapping between 802.1p priorities and queue IDs is as follows: priorities 0 and 1 map queue 1; priorities 2 and 3 map queue 2; priorities 4 and 5 map queue 3; priorities 6 and 7 map queue 4.

5. Save the data.

```
huawei(config)#save
```

- Configure the VoIP service on the OLT.

  1. Create a VLAN and add an upstream port to the VLAN.

     The VLAN ID is 200, and the VLAN is a smart VLAN. The upstream port is0/19/0.

```
huawei(config)#vlan 200 smart
huawei(config)#port vlan 200 0/19 0
```

  2. Configure a traffic profile.

     The traffic profile index is 8, and the 802.1p priority of the VoIP service is 6.

```
huawei(config)#traffic table ip index 8 cir 10240 priority 6 priority-
policy
 local-Setting
```

  3. Configure a service port.

     Add a service port to the VLAN and use traffic profile 8. The user-side VLAN ID is 3.

```
huawei(config)#service-port vlan 200 eth 0/5/2 multi-service user-vlan 3
 rx-cttr 8 tx-cttr 8
```


Copyright © Huawei Technologies Co., Ltd.

```
huawei(config)#service-port vlan 200 eth 0/5/3 multi-service user-vlan 3
 rx-cttr 8 tx-cttr 8
```

4. Configure the DHCP relay.

   The VoIP service and the IPTV service are provided in the DHCP mode. The DHCP option 60 domain is used to differentiate service types.

   - The DHCP domain of the VoIP service is **voice**.
   - The IP addresses of VoIP DHCP server group 1 are 20.1.1.2 and 20.1.1.3.
   - The IP address of the Layer 3 interface of VLAN 200 is 10.1.1.1/24.
   - The gateway IP address of the DHCP domain is 10.1.1.1/24.

```
huawei(config)#dhcp mode layer-3 option-60
huawei(config)#dhcp-server 1 ip 20.1.1.2 20.1.1.3
huawei(config)#dhcp domain voice
huawei(config-dhcp-domain-voice)#dhcp-server 1
huawei(config-dhcp-domain-voice)#quit
huawei(config)#interface vlanif 200
huawei(config-if-vlanif200)#ip address 10.1.1.1 24
huawei(config-if-vlanif200)#dhcp domain voice gateway 10.1.1.1
huawei(config-if-vlanif200)#quit
```

   NOTE

   The DHCP option 60 domain of the Ethernet phone (Ephone) varies with the terminal type. In the actual configuration, see the operation instructions of the Ephone.

5. Save the data.

```
huawei(config)#save
```

- Configure the IPTV service on the OLT.

1. Create a VLAN and add an upstream port to the VLAN.

   The VLAN ID is 1000, and the VLAN is a smart VLAN. The upstream port is0/19/0.

```
huawei(config)#vlan 1000 smart
huawei(config)#port vlan 1000 0/19 0
```

2. Configure a traffic profile.

   The traffic profile index is 9, and the 802.1p priority of the IPTV service is 5.

```
huawei(config)#traffic table ip index 9 cir off priority 5 priority-
policy
 local-Setting
```

3. Configure a service port.

   Add a service port to the VLAN and use traffic profile 9. The user-side VLAN ID is 4.

```
huawei(config)#service-port 200 vlan 1000 eth 0/5/2 multi-service user-
vlan 4
 rx-cttr 9 tx-cttr 9
huawei(config)#service-port 300 vlan 1000 eth 0/5/3 multi-service user-
vlan 4
 rx-cttr 9 tx-cttr 9
```

4. Configure the DHCP relay.

   The VoIP service and the IPTV service are provided in the DHCP mode. The DHCP option 60 domain is used to differentiate service types.

   - The DHCP domain of the IPTV service is **video**.
   - The IP addresses of IPTV DHCP server group 2 are 20.2.2.2 and 20.2.2.3.
   - The IP address of the Layer 3 interface of VLAN 1000 is 10.2.2.1/24.

Copyright © Huawei Technologies Co., Ltd.

- The gateway IP address of the DHCP domain is 10.2.2.1/24.

```
huawei(config)#dhcp mode layer-3 option-60
huawei(config)#dhcp-server 2 ip 20.2.2.2 20.2.2.3
huawei(config)#dhcp domain video
huawei(config-dhcp-domain-video)#dhcp-server 2
huawei(config-dhcp-domain-voice)#quit
huawei(config)#interface vlanif 1000
huawei(config-if-vlanif1000)#ip address 10.2.2.1 24
huawei(config-if-vlanif1000)#dhcp domain video gateway 10.2.2.1
huawei(config-if-vlanif1000)#quit
```

NOTE

The DHCP option 60 domain of the set-top box (STB) varies with the terminal type. In the actual configuration, see the operation instructions of the STB.

5. Create a multicast VLAN and select the IGMP mode.

   Select the IGMP proxy mode.

```
huawei(config)#multicast-vlan 1000
huawei(config-mvlan1000)#igmp mode proxy
  Are you sure to change IGMP mode?(y/n)[n]:y
```

6. Set the IGMP version.

   Set the IGMP version of the multicast VLAN to IGMP v3.

```
huawei(config-mvlan1000)#igmp version v3
```

7. Add an IGMP upstream port.

   The IGMP upstream port is port 0/19/0 and works in the default mode, and protocol packets are transmitted to all the IGMP upstream ports in the multicast VLAN.

```
huawei(config-mvlan1000)#igmp uplink-port 0/19/0
huawei(config-mvlan1000)#btv
huawei(config-btv)#igmp uplink-port-mode default
Are you sure to change the uplink port mode?(y/n)[n]:y
```

8. (Optional) Set the multicast global parameters.

   In this example, the default settings are used for all the multicast global parameters.

9. Configure the program library.

   Configure the program names to BTV-1 and BTV-2, multicast IP addresses of the programs to 224.1.1.10 and 224.1.1.20, and source IP address of the programs to 10.10.10.10.

```
huawei(config-btv)#multicast-vlan 1000
huawei(config-mvlan1000)#igmp program add name BTV-1 ip 224.1.1.10
sourceip
 10.10.10.10
huawei(config-mvlan1000)#igmp program add name BTV-2 ip 224.1.1.20
sourceip
 10.10.10.10
```

10. Configure the right profile.

    Configure the profile name to profile0, with the right of watching program BTV-1.

```
huawei(config-mvlan1000)#btv
huawei(config-btv)#igmp profile add profile-name profile0
huawei(config-btv)#igmp profile profile-name profile0 program-name BTV-1
watch
```

11. Configure the multicast users.

    Add service ports 200 and 300 as multicast users.

```
huawei(config-btv)#igmp user add service-port 200 no-auth
huawei(config-btv)#igmp user add service-port 300 auth
huawei(config-btv)#igmp user bind-profile service-port 300 profile-name
profile0
huawei(config-btv)#multicast-vlan 1000
```


Copyright © Huawei Technologies Co., Ltd.

```
huawei(config-mvlan1000)#igmp multicast-vlan member service-port 200
huawei(config-mvlan1000)#igmp multicast-vlan member service-port 300
huawei(config-mvlan1000)#quit
```

12. Save the data.

```
huawei(config)#save
```

----End

Result

After the related upstream device and downstream device are configured, the triple play service (Internet, VoIP, and IPTV services) is available.

- The Internet user can access the Internet in the PPPoE mode.
- The VoIP user can make and receive phone calls.
- The IPTV user connected to port 0/5/2 can watch all the programs, and the IPTV user connected to port 0/5/3 can watch only program BTV-1.

Configuration File

Internet service:

```
vlan 100 smart
port vlan 100 0/19 0
traffic table ip index 7 cir 10240 priority 1 priority-policy local-Setting
service-port vlan 100 eth 0/5/2 multi-service user-vlan 2 rx-cttr 7 tx-cttr 7
service-port vlan 100 eth 0/5/3 multi-service user-vlan 2 rx-cttr 7 tx-cttr 7
queue-scheduler wrr 10 10 20 20 40 0 0 0
cos-queue-map cos0 0 cos1 1 cos2 2 cos3 3 cos4 4 cos5 5 cos6 6 cos7 7
save
```

VoIP service:

```
vlan 200 smart
port vlan 200 0/19 0
traffic table ip index 8 cir 10240 priority 6 priority-policy local-Setting
service-port vlan 200 eth 0/5/2 multi-service user-vlan 3 rx-cttr 8 tx-cttr 8
service-port vlan 200 eth 0/5/3 multi-service user-vlan 3 rx-cttr 8 tx-cttr 8
dhcp mode layer-3 option-60
dhcp-server 1 ip 20.1.1.2 20.1.1.3
dhcp domain voice
dhcp-server 1
quit
interface vlanif 200
ip address 10.1.1.1 24
dhcp domain voice gateway 10.1.1.1
quit
save
```

IPTV service:

```
vlan 1000 smart
port vlan 1000 0/19 0
traffic table ip index 9 cir off priority 5 priority-policy local-Setting
service-port 200 vlan 1000 eth 0/5/2 multi-service user-vlan 4 rx-cttr 9 tx-cttr 9
service-port 300 vlan 1000 eth 0/5/3 multi-service user-vlan 4 rx-cttr 9 tx-cttr 9
dhcp mode layer-3 option-60
dhcp-server 2 ip 20.2.2.2 20.2.2.3
dhcp domain video
dhcp-server 2
quit
interface vlanif 1000
```


Copyright © Huawei Technologies Co., Ltd.

```
ip address 10.2.2.1 24
dhcp domain video gateway 10.2.2.1
quit
multicast-vlan 1000
igmp mode proxy
y
igmp uplink-port
igmp program add name BTV-1 ip 224.1.1.10 sourceip 10.10.10.10
igmp program add name BTV-2 ip 224.1.1.20 sourceip 10.10.10.10
btv
igmp uplink-port-mode default
y
igmp profile add profile-name profile0
igmp profile profile-name profile0 program-name BTV-1 watch
igmp user add service-port 200 no-auth
igmp user add service-port 300 auth
igmp user bind-profile service-port 300 profile-name profile0
multicast-vlan 1000
igmp multicast-vlan member service-port 200
igmp multicast-vlan member service-port 300
quit
save
```


Copyright © Huawei Technologies Co., Ltd.

10 FTTD Configuration

About This Chapter

This section describes the configurations of Internet access, voice, and video services in fiber to the door (FTTD) networking scenarios.

Context

In FTTD networking scenarios, optical network units (ONUs) connect to user homes through twisted pairs. The ONUs can be installed in shafts or garages, or mounted to courtyard walls.

10.1 FTTD Service Overview
This topic describes FTTD service from basic concepts, network scenarios, typical configurations, and ONU capability sets to provide necessary background information for FTTD service configuration in different scenarios.

10.2 Basic Concepts
This section describes basic concepts related to the fiber to the home (FTTD) solution from the user side to the network side on FTTD networking using PON and P2P upstream transmission, respectively.

10.3 Networking Scenarios and Hardware Configurations (GPON)
This section describes GPON fiber to the door (FTTD) networking scenarios and typical optical line terminal (OLT) and optical network unit (ONU) hardware configurations.

10.4 Reference of GPON ONU Capability Sets
This section provides common Huawei GPON optical network unit (ONU) capability sets, serving as a reference for parameter configuration when an ONU is added offline.

10.5 Principle of FTTD Data Plan

10.6 GPON Access: Configuring FTTD Service
This topic describes how to configure the Internet access service, voice service, BTV service and VoD service in GPON access mode in FTTD network scenario.

Copyright © Huawei Technologies Co., Ltd.

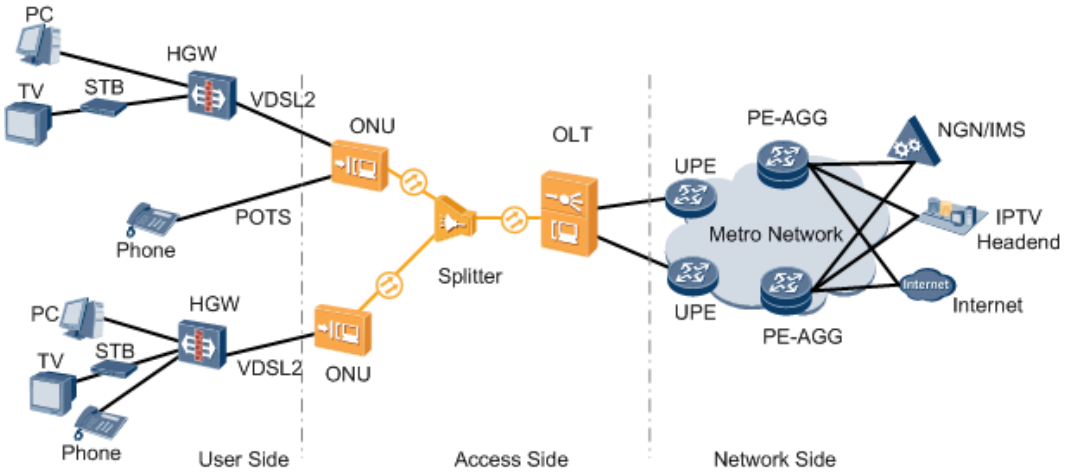
10.1 FTTD Service Overview

This topic describes FTTD service from basic concepts, network scenarios, typical configurations, and ONU capability sets to provide necessary background information for FTTD service configuration in different scenarios.

10.2 Basic Concepts

This section describes basic concepts related to the fiber to the home (FTTD) solution from the user side to the network side on FTTD networking using PON and P2P upstream transmission, respectively.

Integrated FTTD solution networking



Scenario

Concept	Description
Fiber to the door (FTTD)	An optical access scenario where twisted pairs have been deployed at user homes and high bandwidth services are required by the users. The OLT connects to ONUs in the downstream direction through an ODN network. The ONUs can be installed in shafts or garages, or mounted to courtyard walls. The ONUs access users to provide voice, Internet access, and multicast services.

Copyright © Huawei Technologies Co., Ltd.

User Side

Concept	Description
Multicast	Is also called broadband TV (BTV), which is similar to traditional cable TV (CATV) or satellite TV. The user experience in watching a multicast program is the same as that in watching a traditional TV program. Unlike the traditional TV, the IPTV system encodes audio signals and sends them to user terminals through an IP network.
VoD	A technology that enables users to order any program in a VoD program library. During program playing, users can perform operations, such as pause, fast forward, fast rewind, and program locating.

Access Side

Concept	Description
PON	A network that uses the point-to-multipoint (P2MP) network architecture. A PON network consists of an optical line terminal (OLT), an optical distribution network (ODN), and optical network units (ONUs). It uses optical fibers to transmit data, supports more users with less optical fibers, and provides high access rates.
ODN	A network that consists of optical fibers and passive optical components, such as one or more optical dividers. The ODN network provides highly reliable optical paths to connect ONUs to an OLT.
OLT	An aggregation device located at a central office (CO), which terminates PON protocols. In this document. OLTs are MA5600T/MA5603T/ MA5608Ts.
ONU	A user terminal that provides various ports for users. An ONU connects to an OLT for communication through an ODN network.
Split ratio	A ratio used for dividing a downstream optical signal into sub-signals in the PON system. A greater split ratio will result in a high optical power for signal transmission over the same physical distance.
Home gateway (HGW or HG)	A gateway device positioned for small office and home office (SOHO) users. It provides multiple service ports, such as POTS and LAN, wireless local area network (WLAN), or xDSL ports. The HGW supports routing and remote management and diagnosis.

Copyright © Huawei Technologies Co., Ltd.

Network Side

Concept	Description
User-facing provider edge (U-PE)	A supplier routing device that connects to the router of a customer edge (CE), which is an OLT in this document. The U-PE supports routing and Multiprotocol Label Switching (MPLS) encapsulation. If a U-PE connects to multiple CEs, the U-PE supports basic bridging functions. In this case, the U-PE forwards data frames, which reduces the load of switching provider edges (S-PEs).
Aggregation provider edge (PE-AGG)	An aggregation router, which provides aggregation and route forwarding functions for access devices. Compared with U-PEs, PE-AGGs provides fewer ports and higher performance and switching rates.
NGN or IP multimedia subsystem (IMS)	A type of network that centers around softswitches and uses an open and standardized architecture. It provides voice, video, and data services. A type of system that uses Session Initiation Protocol (SIP) signaling as its call control signaling. It provides voice, data, and multimedia services. **NOTE** In this document, the NGN or IMS is the softswitch that supports H.248 or SIP.
IPTV head end	A contents preparation platform in the IPTV system. It receives signals, converts media formats, and manages media materials.

10.3 Networking Scenarios and Hardware Configurations (GPON)

This section describes GPON fiber to the door (FTTD) networking scenarios and typical optical line terminal (OLT) and optical network unit (ONU) hardware configurations.

Copyright © Huawei Technologies Co., Ltd.

Networking Scenario	Description	Typical OLT Configuration	ONU Device
10.6.1 Bridging+Voice ONU Network Scenario (MA5652S)	The ONU integrating an integrated access device (IAD) provides Internet, VoIP, and IPTV services to users. The bridging+voice ONU provides Layer 2 data and voice services. This scenario provides transparent transmission channels and requires simple service configuration, so this scenario applies to Layer 2 networking. ● For data services, a PC or an HGW performs dialup. Then, the upper-layer broadband remote access server (BRAS) device authenticates and accesses the PC. The PC or an HGW can also access the Internet using the Dynamic Host Configuration Protocol (DHCP) or static IP address. ● The ONU with a built-in voice module encapsulates voice service packets, and the OLT transmits them to the upstream next generation network (NGN) or IP multimedia subsystem (IMS).	Typical configuration 1 ● Control board: H801SCUN or H802SCUN ● Service board: H805GPBD, H806GPBH, H802GPBD, or H803GPFD ● Upstream interface board: GICF, GICG, or X2CS Typical configuration 2 ● Control board: H801SCUH ● Service board: HG802GPFD ● Upstream interface board: GICD, GICE, or X2CS	MA5652S
10.6.2 Bridging ONU Network Scenario (MA5651 / MA5651S)	The HGW integrating an IAD provides Internet, voice over Internet Protocol (VoIP), and Internet Protocol television (IPTV) services to users. Services are implemented on the HGW, and the bridging		

Copyright © Huawei Technologies Co., Ltd.

Networking Scenario	Description	Typical OLT Configuration	ONU Device
	ONU works with the OLT to provide Layer 2 channels.		MA5651 or MA5651S

Copyright © Huawei Technologies Co., Ltd.

10.4 Reference of GPON ONU Capability Sets

This section provides common Huawei GPON optical network unit (ONU) capability sets, serving as a reference for parameter configuration when an ONU is added offline.

ONU Type	Product Name	UNI	Number of GEM Ports	IP Address Configured Capability	Number of T-CONTs	Mapping Mode Between Service Streams and the GEM Port	Flow Control Type	Number of PQs Supported by a T-CONT
Bridging ONU +HGW	MA5651 or MA5651S	One VDSL2 port	32	Supported	8	VLAN, PRI, VLAN +PRI, IPToS, or port Port +VLAN, port +PRI, or port +VLAN +PRI	PQ	8
Bridging +voice ONU	MA5652S	One VDSL2 port and two POTS ports	32	Supported	8	VLAN/ PRI/ VLAN +PRI/ IPToS/ Port/ Port +VLAN /Port +PRI/ Port +VLAN +PRI	PQ	8

NOTE

The MA5651 and MA5651S support reverse power supply through the power source equipment (PSE). The MA5652S supports AC power supply.

Copyright © Huawei Technologies Co., Ltd.

10.5 Principle of FTTD Data Plan

10.5.1 Data Plan Principles for IP Addresses

This section describes how to obtain an IP address in various scenarios.

Data Plan Principles for IP Addresses

Terminal Type	Service	Recommended Solution
Bridging +Voice ONU	Internet access	A PC obtains an IP address through PPPoE dialup. The ONU transparently transmits the packets.
	VoIP	The ONU functions as a DHCP client and obtains an IP address from the DHCP server, or the NMS issues a static IP address to the ONU using the configuration file. Voice signaling and media streams at multiple POTS ports share one IP address. Media streams are distinguished by port.
	IPTV	The set top box (STB) obtains an IP address from the DHCP server for ordering programs. The ONU transparently transmits the packets.
Bridging ONU+HGW	Internet access	The HGW functions as a PPPoE client and obtains an IP address through PPPoE dialup. At the same time, the HGW functions as a DHCP server and allocates IP addresses to PCs through the network cable and wireless fidelity (Wi-Fi) access. The ONU transparently transmits the packets.
	VoIP	The HGW functions as a DHCP client and obtains an IP address from the DHCP server, or the application control server (ACS) issues a static IP address to the HGW using TR069. Voice signaling and media streams at multiple POTS ports share one IP address. Media streams are distinguished by port. The ONU transparently transmits the packets.
	IPTV	The HGW is configured with a bridging WAN port. The STB obtains an IP address from the DHCP server. The HGW transparently transmits packets. The ONU also transparently transmits the packets.

10.5.2 Principle of QoS Planning

The QoS planning is an E2E planning, and it can be divided into following policies: traffic classification, marking, and scheduling policy; and traffic monitoring and DBA policy.

Copyright © Huawei Technologies Co., Ltd.

Traffic Classification, Marking, and Scheduling Policy

Service Type	802.1p Priority	Queue Scheduling Method	OLT Queue ID (8 Queues)	ONU Queue.ID	
				When Eight Queues Are Supported	When Four Queues Are Supported
Management service	6	PQ	6	6	3
VoIP service	5	PQ	5	5	2
IPTV service	4	PQ	4	4	2
Internet access service	0	PQ	0	0	0

Note: The service priorities in this table are the recommended values. The service priorities are arranged according to the operators's actual plan.

Traffic Monitoring and DBA Policy

Items	Management service	Internet access service	VoIP service	IPTV service
GEM port	11 [Remark 1]	12	13	14
TCONT	All services share a T-CONT.			
DBA type	Type 3 (DBA profile: assured bandwidth + maximum bandwidth. Users are allowed to preempt the bandwidth on condition that the users' assured bandwidth is guaranteed. However, the total bandwidth cannot exceed the maximum bandwidth.)			
DBA bandwidth planning	Configure the DBA bandwidth according to the user's bandwidth package. The assured bandwidth is the maximum bandwidth required by management packets, VoIP, and IPTV upstream packets. The maximum bandwidth is larger than or equal to the maximum bandwidth that users apply.			
Rate limit on OLT downstream	No rate limit	Configure rate limit by a traffic profile as required. [Remark 2]	No rate limit	No rate limit

Copyright © Huawei Technologies Co., Ltd.

Items	Management service	Internet access service	VoIP service	IPTV service
Rate limit on ONU upstream port	No rate restriction			
Rate limit on ONU downstream port	No rate restriction			

Remark 1: GEM port value depends on the planning of the service provider, but in principle, use different GEM ports for different services.

Remark 2: **Table 10-1** shows the reference service bandwidth of each service for each user.

Table 10-1 Reference service bandwidth of each service for each user

Service Type	Upstream Bandwidth	Downstream Bandwidth	Bandwidth Description
Internet access service	Determined based on the service tariff package.	Determined based on the service tariff package.	Available bandwidth or Internet access service = Committed bandwidth of the service tariff package - VoIP bandwidth - IPTV bandwidth
VoIP service	200 kbit/s	200 kbit/s	The upstream bandwidth and the downstream bandwidth of VoIP service are symmetrical. The actual bandwidth is related to the coding format. This bandwidth is calculated for two POTS ports.
IPTV service (standard definition program)	/	2.5 Mbit/s per channel	IPTV service mainly occupies the downstream bandwidth. The actual bandwidth depends on the coding format, the picture in picture information, 10% bandwidth burst traffic, and the number of programs that can be concurrently watched by one user (in the case of multiple STBs). The upstream bandwidth is mainly used for transmitting IGMP packets, which requires little bandwidth. Therefore, the bandwidth occupied by IGMP packets can be neglected.

Copyright © Huawei Technologies Co., Ltd.

Service Type	Upstream Bandwidth	Downstream Bandwidth	Bandwidth Description
IPTV service (high definition program)	/	9.7 Mbit/s per channel	

Note:

- The rate restriction on the BRAS or SR is recommended. OLTs and ONUs do not restrict the rate for service streams.
- If BRAS does not support rate restriction, OLTs can restrict the rate for service streams through the traffic profile.
- Different service packets on the ONU are distinguished by different VLAN IDs. The service packets are mapped to GEM ports based on VLAN IDs so that different service packets are transmitted to different GEM ports. Each GEM port (each service) corresponds to a T-CONT or all GEM ports share a T-CONT.
- The sum of the assured bandwidth of all ONUs connected to a PON port and the fixed bandwidth of OMCI management channel is less than the GPON upstream bandwidth. Some bandwidth must be reserved for the future service expansion.

10.5.3 Principle of Internet Access Service Data Plan

The Internet access service plan mainly includes the plan of the VLAN and VLAN translation policy in different network scenarios.

VLAN and VLAN Translation policy.

Application Scenario	VLAN Plan	VLAN Translation Policy
Bridging ONU	Double-tagged VLAN	ONU: ONUs configure the VLAN and add the same C-VLAN tag to packets. All ONUs are in the same C-VLAN. OLT: The OLT performs VLAN translation: C<->S+C'. The C'-VLAN of every ONU differs from each other.

Copyright © Huawei Technologies Co., Ltd.

Application Scenario	VLAN Plan	VLAN Translation Policy
Bridging ONU + HGW	Double-tagged VLAN	ONU: The upstream packets sent from the HGW carry user-VLANs and the ONU transparently transmits them. OLT: The OLT translates the U-VLAN to S-VLAN+C-VLAN.

Note:

- UserVLAN: VLAN carried by upstream packets of user-side devices, U for short.
- C-VLAN: VLAN added based on the ONU port. For details, see the description of the Double-tagged VLAN S+C.
- Double-tagged VLAN S+C: C indicates the inner VLAN (C-VLAN) and S indicates the outer VLAN (S-VLAN).
- Double-layer VLAN S+C': C' indicates the translated inner VLAN (C'-VLAN) and S indicates the outer VLAN (SVLAN).
- Single-tagged S-VLAN: Single-tagged VLAN marked or translated by the OLT. It is generally used in a single-tagged VLAN translation scenario.
- C<->S+C': Bidirectional VLAN translation: translates the inner C-VLAN and then adds one outer S-VLAN.
- C<->S+C: Bidirectional VLAN translation: maintains the inner C-VLAN and adds one outer S-VLAN.

NOTE

- To ensure traceability of users and finer-grained QoS control and management of users and services, plan per user per service per VLAN (PUPSPV) for the Internet access service. Considering OLT capacity and VLAN scalability, use dual VLANs (S-VLAN+C-VLAN) on the OLT to differentiate users for the Internet access service.
- The outer S-VLAN, which identifies services and physical location, can be allocated based on the OLT, PON board, or PON port. The inner C-VLAN identifies users. User C-VLANs must be unique in one S-VLAN.
- It is recommended that you use stacking VLANs as S-VLANs so that security features, such as PPPoE+/ opton82, and anti MAC attacks and anti spoofing spoofing can be easily deployed.
- The 802.1q in 802.1q (QinQ) VLAN is used in the enterprise private line scenario, such as (TLS). The device transparently transmits packets. It is not recommended that you use QinQ VLANs as S-VLANs for the triple play services of residential users.

10.5.4 Principle of Voice Service Data Plan

The voice service plan mainly includes the plan of the VLAN and VLAN translation policy in different network scenario, and the plan of voice protocol.

Copyright © Huawei Technologies Co., Ltd.

VLAN and VLAN Translation Policy.

Application Scenario	VLAN Plan	VLAN Translation Policy
Bridging + Voice ONU	Single-tagged VLAN	ONU: ONUs provide the VoIP service and use the same S-VLAN.
	Double-tagged VLAN	ONU: ONUs provide the VoIP service and use the same C-VLAN. The C-VLAN identifies the VoIP service. OLT: The OLT adds S-VLANs to packets. The C-VLAN is translated to S-VLAN+C-VLAN.
Bridging ONU + HGW	Single-tagged VLAN	ONU: transparently transmits the user VLAN tags carried in the upstream packets sent from the HGW. OLT: translates user VLAN tags to S-VLAN tags.
	Double-tagged VLAN	ONU: transparently transmits the user VLAN tags carried in the upstream packets sent from the HGW. OLT: translates the user VLAN tags to S-VLAN+C-VLAN tags.

NOTE

- The VoIP service is a closed service self-operated by carriers. The single-tagged S-VLAN is the mainstream application and is recommended.
- When the planned VLAN is single-tagged VLAN, the S-VLAN can identify services and physical locations based on an OLT device, a PON board or a PON port. It is recommended that you set different voice VLANs for the OLTs connected to one VoIP SR to avoid an excessively large broadcast domain of the SR and convergence switch.
- When the planned VLAN is S-VLAN+C-VLAN, the outer S-VLAN can identify services and physical locations based on an OLT device, a PON board or a PON port. The inner C-VLAN is used to identify services (the fixed value) and users.

VoIP Data Plan Based on H.248 or SIP

Item			Description
MG interface/ SIP interface data	Media and signaling parameters	Media and signaling upstream VLANs	Upstream VLANs of the VoIP service
		Media and signaling uplink port	Uplink ports of the VoIP service

Copyright © Huawei Technologies Co., Ltd.

Item			Description
NOTE must be consistent with the data on the MGC/IMS core network devices.		Media IP addresses and signaling IP addresses	Supports separating media from signaling.
		Default gateway IP address.	The next hop IP address from an ONU/HGW to an MGC/IMS.
	MG interface/SIP interface ID		None
	Signaling port ID		Choose the transmission mode according to the requirement of the MGC/IMS side.
	IP address of active MGC (H.248)/IP address of active IMS device (SIP)		If the dual homing is not configured, only one MGC parameter needs to be configured. If the dual homing is configured, the IP address and port ID of the standby MGC need to be configured.
	Port ID of active MGC (H248)/ port ID of active IMS device (SIP)		
	Coding		Choose the coding method according to the requirement on the MGC/IMS side. Generally, the text coding method is adopted.
	Transmission mode		Choose the transmission mode according to the requirement on the MGC/IMS side. Generally, the UDP transmission mode is adopted.
	Home domain (SIP)		None
	Profile index		None
	The version of H248 protocol that MG starts to negotiate		V1, V2 or V3 (by default). The interface may fail to be registered because some softswitches do not support V3.
Voice user data	Phone number		For H248 protocol: The phone numbers allocated by the MGC need to be determined, and the paging numbers for users' emergency standalone need to be planned if the emergency standalone function is provided. For SIP protocol: The phone number that the IMS core network device allocates to the user must be configured.
	Terminal ID (H248)		If the TID template with which the POTS user is bound does not support terminal layering, this parameter needs to be configured.

Copyright © Huawei Technologies Co., Ltd.

Item		Description
	User priority	According to the service requirements, user priorities must be specified. The user priorities include the following: ● cat1: government1 (category 1 government users) ● cat2: government2 (category 2 government users) ● cat3: common (common users)
	User type	According to the service requirements, user type needs to be specified. The user type includes the following: ● DEL: direct exchange lines (default) ● ECPBX: earth calling PBX ● LCPBX: loop calling PBX ● PayPhone: pay phone
	Public port parameters	Include the fax mode, fax or modem negotiation mode, and codec mode priority.
	POTS port attributes	Include the impedance, TX gain, RX gain, and signaling type of a POTS port.

10.5.5 Principle of IPTV Service Data Plan

The IPTV service data plan mainly include the plan of VLAN and VLAN translation policy in different network scenario, and the plan of IPTV service.

VLAN and VLAN Translation Policy.

Application Scenario	Service Type	VLAN Plan	VLAN Translation Policy
Bridging ONU	Multicast service	Single-tagged VLAN	ONUs replicate multicast packets based on user ports and multicast VLANs (M-VLANs) are removed downstream. The OLT replicates multicast packets based on PON ports with M-VLAN unchanged.
	VoD	Single-tagged VLAN	ONUs add S-VLAN tags to iTV service packets. The OLT transparently transmits packets with S-VLANs.

Copyright © Huawei Technologies Co., Ltd.

Application Scenario	Service Type	VLAN Plan	VLAN Translation Policy
		Double-tagged VLAN	All ONUs add the same C-VLAN tag to packets. The OLT implements VLAN translation: C->S+C'.
Bridging ONU + HGW	Multicast service	Single-tagged VLAN	ONUs transparently transmit upstream packets with M-VLANs sent from HGW. Multicast packets are replicated downstream with M-VLAN unchanged. The OLT replicates multicast packets based on PON ports with M-VLAN unchanged.
		Single-tagged VLAN	ONUs translate the upstream VLANs sent from HGW to M-VLANs. The OLT replicates multicast packets based on PON ports with M-VLAN unchanged.
	VoD	Single-tagged VLAN	ONUs transparently transmit the upstream U-VLANs sent from HGW. The OLT implements VLAN translation: U->S.
		Double-tagged VLAN	ONUs transparently transmit the upstream U-VLANs sent from HGW. The OLT implements VLAN translation: U->S+C.

Note:

- UserVLAN: VLAN carried by upstream packets of user-side devices, U for short.
- C-VLAN: VLAN added based on the ONU/ONU port. For details, see the description of the Double-tagged VLAN S+C.
- Double-tagged VLAN S+C: C indicates the inner VLAN (C-VLAN) and S indicates the outer VLAN (S-VLAN).
- Double-layer VLAN S+C': C' indicates the translated inner VLAN (C'-VLAN) and S indicates the outer VLAN (SVLAN).
- Single-tagged S-VLAN: Single-tagged VLAN marked or translated by the OLT. It is generally used in a single-tagged VLAN translation scenario.
- C<->S+C': Bidirectional VLAN translation: translates the inner C-VLAN and then adds one outer S-VLAN.
- C<->S+C: Bidirectional VLAN translation: maintains the inner C-VLAN and adds one outer S-VLAN.

Copyright © Huawei Technologies Co., Ltd.

NOTE

- IPTV service is a closed service self-operated by carriers, and single-tagged S-VLAN is recommended.
- The same S-VLAN or different S-VLANs can be used as the M-VLAN and VoD VLAN. It is recommended that you use different S-VLANs as M-VLAN and VoD VLAN so that the upper-level device easily differentiates between the BTV service and VoD service.
- S-VLANs of VoD service can identify services and physical locations based on an entire network or an OLT. It is recommended that you set different VoIP VLANs for the OLTs connected to one VoIP SR to avoid an excessively large broadcast domain of the VoIP SR and convergence switch.

10.6 GPON Access: Configuring FTTD Service

This topic describes how to configure the Internet access service, voice service, BTV service and VoD service in GPON access mode in FTTD network scenario.

Context

There are two GPON configuration modes: distributed mode (also called discrete mode) and profile mode. The difference between the two modes lies in command lines.

- Distributed mode: In this mode, ONUs need to be configured one by one but not in batches.
- Profile mode: In this mode, an ONU line profile and service profile are configured first. Then, ONUs can be added in batches by binding profiles. This mode greatly improves service provisioning efficiency.

Generally, the GPON configuration mode is determined in a new deployment and will not be changed. This chapter describes how to configure the enterprise access service in PON profile mode (which is the default mode). You can run the commands in the following table to query the GPON configuration mode.

Mode	Query Method
PON profile mode	huawei(config)#**diagnose** huawei(diagnose)%%**display xpon mode** --- Current config mode: Profile-mode ---

NOTE

For commands for the distributed configuration mode, see **PON distributed-mode commands** in the *Command Reference*.

10.6.1 Bridging+Voice ONU Network Scenario (MA5652S)

This topic describes how to configure Internet access service, voice service, BTV service and VoD service when bridging+voice ONUs are used to build an FTTD network.

Copyright © Huawei Technologies Co., Ltd.

10.6.1.1 Service Requirements and Application Scenario

Service Requirements

Optical fibers are connected to user homes and triple play services are required. The following provides detailed service requirements:

- Internet access of multiple PCs in a home is supported.
- Access of multiple telephones in a home is supported.
- IPTV programs can be previewed and watched using STBs.
- Service extension is supported and different services do not affect each other.
- Proper service security is ensured.
  - Internet access services are protected against unauthorized access, and malicious attacks.
  - Voice and IPTV services are protected against malicious attack, and traffic flooding attacks.
- Service faults are easy to locate and services are easy to maintain.

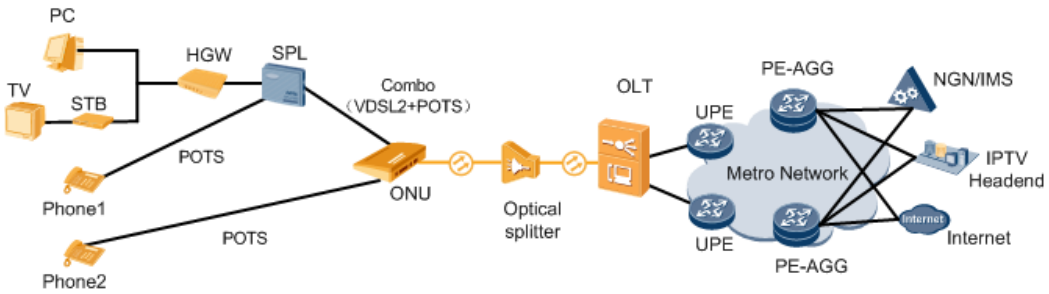
Application Scenario

As shown in **Figure 10-1**, the ONU integrating an integrated access device (IAD) provides Internet, VoIP, and IPTV services to users.

The bridging+voice ONU provides Layer 2 data and voice services. This scenario provides transparent transmission channels and requires simple service configuration, so this scenario applies to Layer 2 networking.

- For data services, a PC directly performs dial-up. Then, the upper-layer broadband remote access server (BRAS) device authenticates and accesses the PC. The PC can also access the Internet using the Dynamic Host Configuration Protocol (DHCP) or static IP address.
- The ONU with a bulit-in voice module encapsulates voice service packets, and the OLT transmits them to the upstream next generation network (NGN) or IP multimedia subsystem (IMS).

Figure 10-1 Bridging+Voice ONU

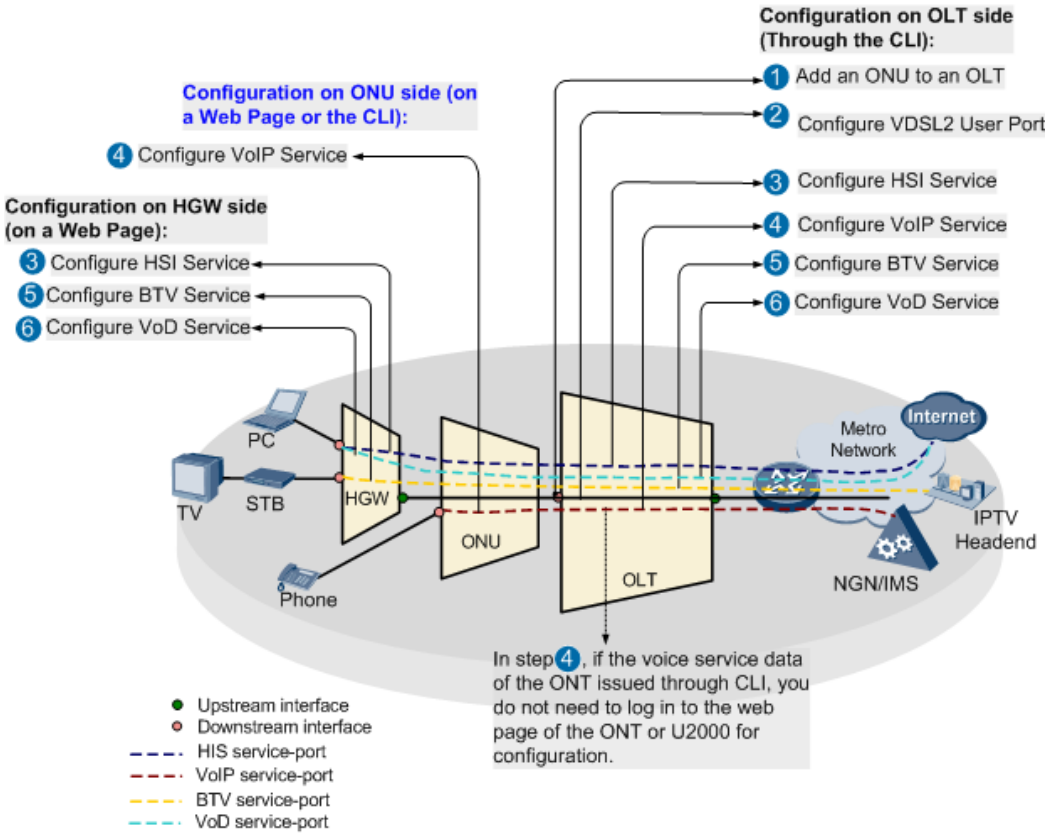


10.6.1.2 Configuration Process

Figure 10-2 shows the configuration roadmap in fiber to the door (FTTD) networking using a bridging+voice optical network unit(ONU).

Copyright © Huawei Technologies Co., Ltd.

Figure 10-2 Configuration roadmap in FTTD networking using a bridging+voice ONU



The following table describes the configuration steps.

Item	Step	Description
Optical line terminal (OLT)	**10.6.1.3 Adding an ONU to an OLT**	Services can be configured for an optical network unit (ONU) only after the ONU is added to an optical line terminal (OLT).
OLT	**10.6.1.4 Configuring a VDSL2 User Port**	Services can be transmitted only after a VDSL2 port on an optical network unit (ONU) is activated.
OLT HGW	**10.6.1.5 Configuring the Internet Access Service**	None

Copyright © Huawei Technologies Co., Ltd.

Item	Step		Description

OLT
ONU
U2000
	Configure the VoIP service.	**10.6.1.6 Configuring the H.248-based Voice Service (Through the CLI)**	**NOTE**
			● The H.248 and Session Initiation Protocol (SIP) protocols are mutually exclusive for the VoIP service. Either of them is configured at a time.
			● The voice service can be configured through command line interface (CLI) on an OLT, web page, or U2000. Select a configuration mode based on site requirements.
			  ● OLT CLI: This mode can be used for site deployment or the U2000 has not been deployed.
			  ● Web page: This mode can be used to configure voice parameters after the service channel has been configured through the OLT CLI. It can be used for site deployment.
			  ● U2000: This mode can be used to configure voice parameters after the service channel has been configured through the OLT CLI. It can be used for service provisioning in batches.

		10.6.1.7 Configuring the H.248-based Voice Service (on a Web Page)	
		10.6.1.8 Configuring the SIP-based Voice Service (Through the CLI)	
		10.6.1.9 Configuring the SIP-based Voice Service (on a Web Page)	
OLT HGW	Configure the IPTV service.	**10.6.1.10 Configuring the BTV Service**	IPTV services include the BTV and VoD services that are different in configuration procedures and need to be configured separately.
		10.6.1.11 Configuring the VoD Service	
OLT	**10.6.1.12 Verifying Services**		The OLT provides remote verification methods including ONU PPPoE/DHCP dialup emulation and call emulation for configuration and commissioning engineers to verify services remotely after service configuration, avoiding a second on-site operation.

Copyright © Huawei Technologies Co., Ltd.

10.6.1.3 Adding an ONU to an OLT

Services can be configured for an optical network unit (ONU) only after the ONU is added to an optical line terminal (OLT).

Data Plan

Table 10-2 Data plan

Item	Data
DBA profile	Profile name: fttd_dba Profile type: type3 Assured bandwidth: 8 Mbit/s Maximum bandwidth: 20 Mbit/s
ONU line profile	Profile name: fttd T-CONT ID: 4 GEM port ID for the management service: 11 GEM port ID for the voice service: 12 GEM port ID for the video service: 13 GEM port ID for the Internet access service: 14
ONU service profile	Profile name: fttd ONU port capability set: one VSDL2 port and two POTS ports
Network topology data	PON port: 0/1/0 ONU IDs: 1

Procedure

Step 1 Configure GPON ONU profiles.

GPON ONU profiles include the DBA profile, line profile, service profile, and alarm profile.

- DBA profile: A DBA profile describes GPON traffic parameters. A T-CONT is bound to a DBA profile for dynamic bandwidth allocation, improving upstream bandwidth utilization.
- Line profile: A line profile describes the binding between the T-CONT and the DBA profile, the QoS mode of the traffic stream, and the mapping between the GEM port and the ONU-side service.
- Service profile: A service profile provides the service configuration channel for the ONU that is managed by using optical network terminal management and control interface (OMCI).
- Alarm profile: An alarm profile contains a series of alarm thresholds to measure and monitor the performance of activated ONU lines. When a statistical value reaches the threshold, the host is notified and an alarm is reported to the log host and the NMS.

1. Configure a DBA profile.

Copyright © Huawei Technologies Co., Ltd.

Run the **display dba-profile** command to query existing DBA profiles in the system. If the existing DBA profiles in the system do not meet the requirements, run the **dba-profile add** command to add a DBA profile.

Create the same DBA profile for different types of services. Set the profile name to **fttd_dba**, profile type to **type3**, assured bandwidth to 8 Mbit/s, and maximum bandwidth to 20 Mbit/s.

```
huawei(config)#dba-profile add profile-name fttd_dba type3 assure 8192 max
20480
```

NOTE

The DBA implementation is based on an ONU. Therefore, select a DBA profile of the proper bandwidth type and configure proper bandwidth according to the service types and total user count of the ONU. Note that the sum of the fixed bandwidth and the assured bandwidth must not be greater than the total bandwidth of the PON port.

2. Configure an ONU line profile.

   Create a GPON ONU line profile, named **fttd**, and bind it to the DBA profile **fttd_dba**.

   ```
   huawei(config)#ont-lineprofile gpon profile-name fttd
   huawei(config-gpon-lineprofile-1)#tcont 4 dba-profile-name fttd_dba
   ```

   Create different GEM ports according to different service types, in which

   - GEM port 11 is used to carry management services.
   - GEM port 12 is used to carry voice services.
   - GEM port 13 is used to carry video services.
   - GEM port 14 is used to carry Internet access services.

   ```
   huawei(config-gpon-lineprofile-1)#gem add 11 eth tcont 4
   huawei(config-gpon-lineprofile-1)#gem add 12 eth tcont 4
   huawei(config-gpon-lineprofile-1)#gem add 13 eth tcont 4
   huawei(config-gpon-lineprofile-1)#gem add 14 eth tcont 4
   ```

   NOTE

   1. To change the default QoS mode, run the **qos-mode** command to set the QoS mode to **gem-car** or **flow-car**, and run the **gem add** command to set the index of the traffic profile bound to the GEM port.
   2. When the QoS mode is priority-queue (PQ), the default queue priority is 0; when the QoS mode is flow-car or gem-car, traffic profile 6 is bound to the GEM port by default (no rate limitation).

   After the configurations are complete, run the **commit** command to apply the parameter settings.

   ```
   huawei(config-gpon-lineprofile-1)#commit
   huawei(config-gpon-lineprofile-1)#quit
   ```

3. Configure an ONU service profile.

   Create a GPON ONU service profile, named **fttd**. Configure the capability set of the VDSL2 port and POTS port to **1** and **2**. Then the system automatically adapts to the ONU according to the actual capability of the online ONU.

   ```
   huawei(config)#ont-srvprofile gpon profile-name fttd
   huawei(config-gpon-srvprofile-1)#ont-port vdsl 1 pots 2
   ```

   After the configurations are complete, run the **commit** command to apply the parameter settings.

   ```
   huawei(config-gpon-srvprofile-1)#commit
   huawei(config-gpon-srvprofile-1)#quit
   ```

4. (Optional) Add an alarm profile.

   - The default GPON alarm profile 1 is used. The alarm thresholds of the default alarm profile are 0, which indicates that no alarm is generated.

Copyright © Huawei Technologies Co., Ltd.

- In this example, the default alarm profile is used, and therefore the configuration of the alarm profile is not required.
- Run the **gpon alarm-profile add** command to configure a GPON alarm profile, which is used for monitoring the performance of an activated ONU line.

Step 2 Add an ONU.

Connect an ONU to GPON port 0/1/0. Set the ONU ID to **1**, password to **0100000001**, discovery mode for password authentication to **once-on**, and management mode to **OMCI**. Bind the ONU to ONU line profile **fttd** and ONU service profile **fttd**.

There are two methods of adding an ONU: add an ONU offline and confirm an automatically discovered ONU.

- Add ONUs offline.

  If the password of an ONU is known, run the **ont add** command to add an ONU offline.

```
huawei(config)#interface gpon 0/1
huawei(config-if-gpon-0/1)#ont add 0 1 password-auth 0100000001 once-on no-aging
omci ont-lineprofile-name
 fttd ont-srvprofile-name fttd
```

- Confirm automatically discovered ONUs

  If the password or SN of an ONU is unknown, run the **port *portid* ont-auto-find enable** command in GPON mode to enable the ONU auto-discovery function of the GPON port. Then, run the **ont confirm** command to confirm the ONU.

```
huawei(config)#interface gpon 0/1
huawei(config-if-gpon-0/1)#port 0 ont-auto-find enable
huawei(config-if-gpon-0/1)#display ont autofind 0
  //After this command is executed, the information about all ONUs connected to
the GPON port through optical splitters is displayed.

huawei(config-if-gpon-0/1)#ont confirm 0 ontid 1 password-auth 0100000001 once-
on no-aging omci ont-lineprofile-name
 fttd ont-srvprofile-name fttd
```

NOTE

If multiple ONUs of the same type bound to the same line profile or service profile are connected to the same port, you can bulk add ONUs by bulk confirming automatically discovered ONUs to make configuration easier and more efficient. To do so, the preceding command can be modified as follows:

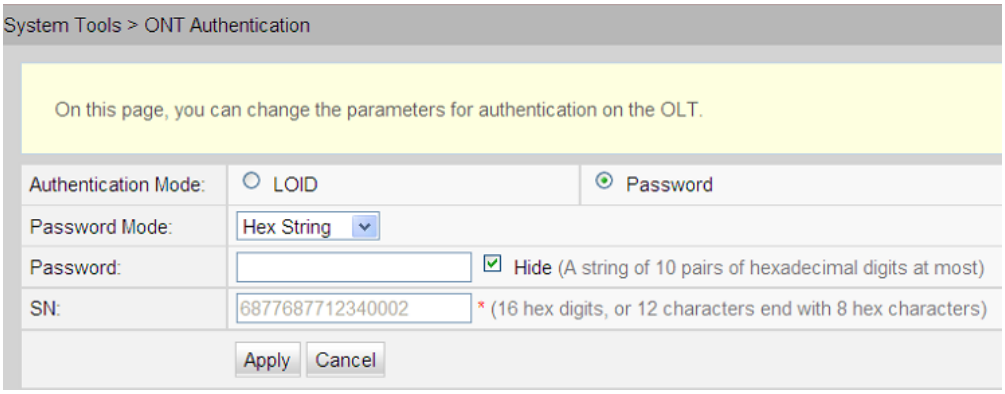
```
huawei(config-if-gpon-0/1)#ont confirm 0 all password-auth once-on no-agin omci
ont-lineprofile-name fttd
ont-srvprofile-name fttd
```

NOTE

The password entered when you add an ONU to the OLT must be the same as that configured on the web page. To configure the password of the ONU on the web page, see **Figure 10-3**.

Copyright © Huawei Technologies Co., Ltd.

Figure 10-3 Modifying ONU password on the web page



- (Optional) Bind the alarm profile to the ONU.

  The default profile 1 is used in this example.

  ```
  huawei(config-if-gpon-0/1)#ont alarm-profile 0 1 profile-id 1
  ```

Step 3 Check ONU status.

After an ONU is added, run the **display ont info** command to query the current status of the ONU. Ensure that **Config flag** of the ONU is **active**, **Run State** is **online**, **Config state** is **normal**, and **Match state** is **match**.

```
huawei(config-if-gpon-0/1)#display ont info 0 1
  ------------------------------------------------------------------------
  F/S/P                   : 0/1/0
  ONU-ID                  : 1
  Control flag            : active    //Indicates that the ONU is
activated.
  Run state               : online    //Indicates that the ONU goes online
successfully.
  Config state            : normal    //Indicates that the configuration state of the
ONU is normal.
  Match state             : match     //Indicates that the capability profile bound to
the ONU is consistent with the actual capability of the ONU.
...//The rest of the response information is omitted.
```

When **Config state** is **failed**, **Run state** is **offline**, or **Match state** is **mismatch**:

- If **Control flag** is **deactive**, run the **ont active** command in GPON mode to activate the ONU.
- If **Run state** is **offline**, a physical line may be broken or the optical module may be damaged. Check the line and the optical module.
- If **Config state** is **failed**, the configured ONU capability exceeds the actual ONU capability. In this case, run the **display ont failed-configuration** command in the diagnose mode to check the failed configuration item and the failure cause. Then, rectify the fault accordingly.

----End

10.6.1.4 Configuring a VDSL2 User Port

Services can be transmitted only after a VDSL2 port is activated on an optical network unit (ONU). This section describes how to activate a VDSL2 port and bind a VSDL2 line profile to the port.

Copyright © Huawei Technologies Co., Ltd.

Prerequisites

- An ONU has been added to the optical line terminal (OLT). For details, see **10.6.1.3 Adding an ONU to an OLT**.
- Run the **display xdsl mode** command to check whether the VDSL2 mode is the desired mode. The default mode is TR129. If the current mode is not the desired one, run the **switch vdsl mode to** command in diagnose mode to switch the mode to the desired mode.

  NOTE

  - A fiber to the door (FTTD) network supports only the TR129 and TR165 modes.
  - G.INP takes effect preferentially if both G.INP and SRA are enabled.

Typical VDSL2 Line Parameter Configurations

Key parameters to be configured do not vary with the VDSL2 mode but belong to different profiles. Hence, commands for configuring the key parameters vary with the VDSL2 mode.

Table 10-3 lists the typical configurations for key parameters of a VDSL2 line (26 AWG, 0.4 mm twisted pair). Information provided in this table is for reference only. Usually, take the default values for the other parameters.

Table 10-3 Typical configurations for key parameters of a VDSL2 line (0.4 mm twisted pair)

Parameter	Access Distance					Remarks
	< 100 m	< 300 m	300-500 m	500-800 m	800-1000 m	
Selected VDSL2 profile	30a	17a	12a	8b, 12a	8b	A 30a VDSL2 profile is recommended on an FTTD network.
PSD mask	B8-16 (998-M2x-B)	B8-11 (998ADE17-M2x-A)	B8-6 (998-M2x-B)	B8-6 (998-M2x-B)	B8-6 (998-M2x-B)	None
Enable US0 (U0)	No	Yes	Yes	Yes	Yes	Enable US0 if the distance is longer than 500 m.
Maximum transmit rate downstream	100 Mbit/s	50 Mbit/s	40 Mbit/s	25 Mbit/s	20 Mbit/s	● Limiting the upstream and downstream rates ensures a higher signal-to-

Copyright © Huawei Technologies Co., Ltd.

Parameter	Access Distance					Remarks
	< 100 m	< 300 m	300-500 m	500-800 m	800-1000 m	
Maximum transmit rate upstream	15 Mbit/s	15 Mbit/s	10 Mbit/s	5 Mbit/s	2 Mbit/s	noise ratio (SNR) margin for the line and therefore enhances its capability for withstanding noise and interference. ● The rates can be specified using these two parameters and also can be specified in the traffic profile. When they are specified in both ways, the actual activation rate is determined by the smaller one.
Minimum INP	2 symbols	2 symbols	2 symbols	2 symbols	2 symbols	None
Target SNR margin	8 dB	8 dB	8 dB	8 dB	8 dB	None

Copyright © Huawei Technologies Co., Ltd.

Parameter	Access Distance					Remarks
	< 100 m	< 300 m	300-500 m	500-800 m	800-1000 m	
Path mode	PTM	PTM	PTM	PTM	PTM	Only the PTM mode is supported on an FTTD network.

Configuration Process

Figure 10-4 shows the process for configuring a VDSL2 line profile in TR129 mode.

Figure 10-4 Flowchart for configuring a VDSL2 line profile in TR129 mode

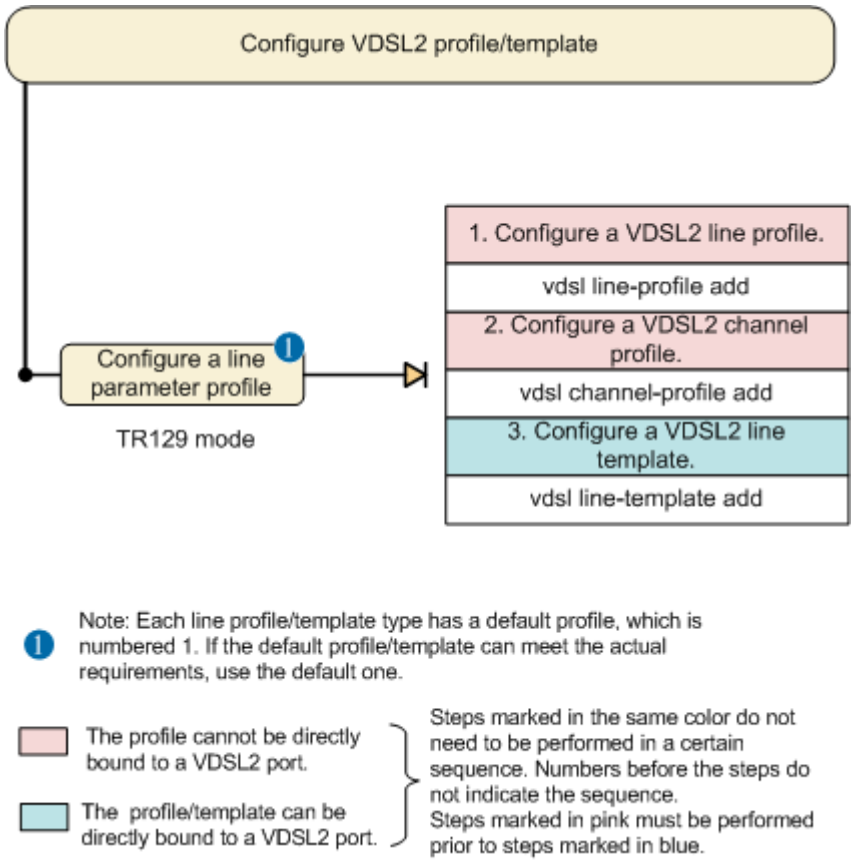
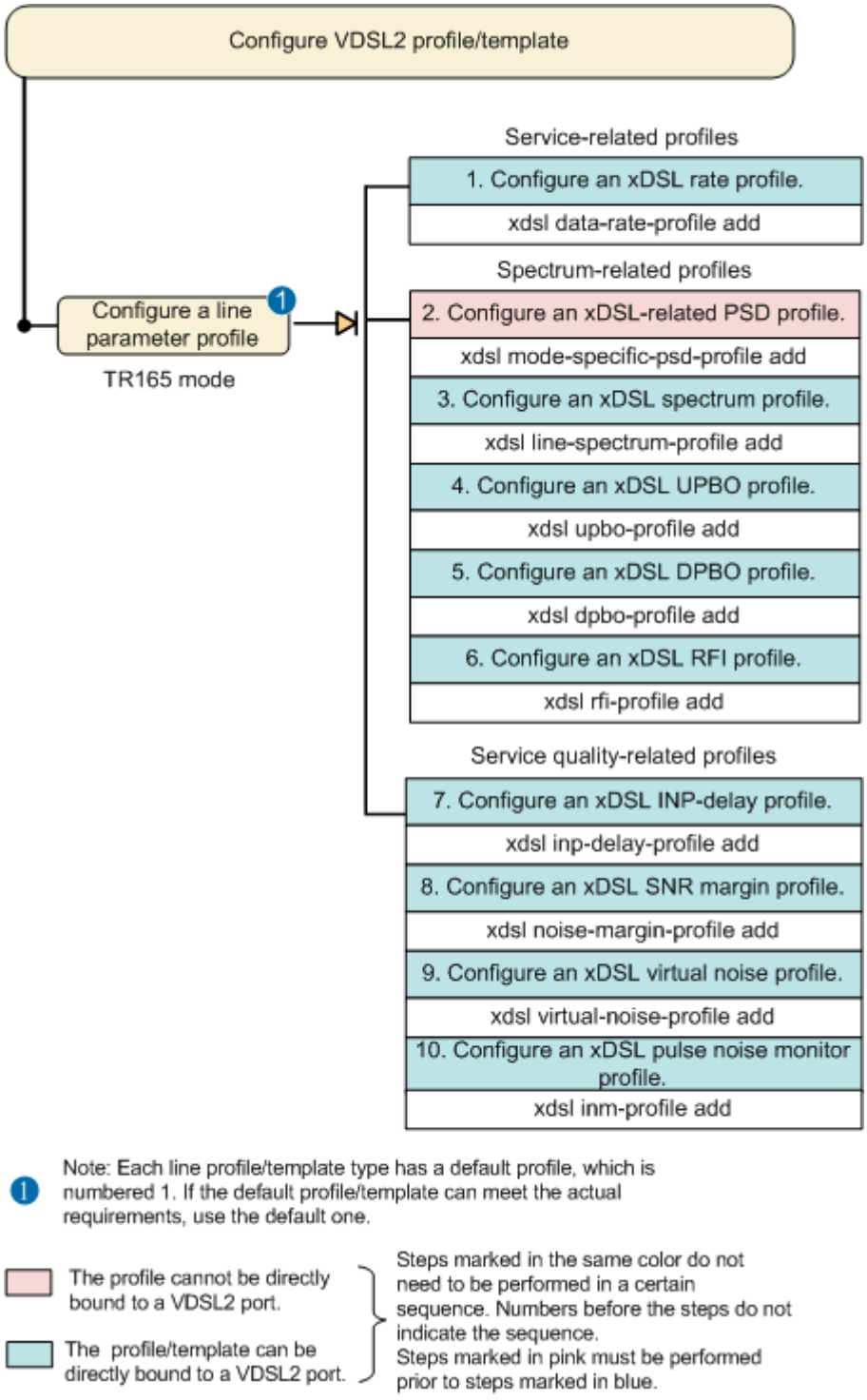


Figure 10-5 shows the process for configuring a VDSL2 line profile in TR165 mode.

Copyright © Huawei Technologies Co., Ltd.

Figure 10-5 Flowchart for configuring a VDSL2 line profile in TR165 mode



Procedure

Step 1 (Optional) Run the command in **Figure 10-4** or **Figure 10-5** to configure a VDSL2 line profile.

Copyright © Huawei Technologies Co., Ltd.

Perform this step if the default line profile (ID: 1) cannot meet site requirements. In this section, the default line profile is used.

Step 2 Activate a VDSL2 port and bind the VDSL2 line profile to the port.

Perform this step after the ONU becomes functional. The PON port data is shown in the following table.

Networking data	PON port: 0/1/0
	ONU ID: 1

In TR129 mode:

```
huawei(config-if-gpon-0/1)#ont port activate 0 1 vdsl-port 1 template-index 1
```

In TR165 mode:

```
huawei(config-if-gpon-0/1)#ont port activate 0 1 vdsl-port 1
```

----End

10.6.1.5 Configuring the Internet Access Service

An optical line terminal (OLT) is connected to a remote optical network unit (ONU) through a GPON port to provide users with high-speed Internet access services.

Prerequisites

- The OLT is connected to the BRAS.
- Related configurations are performed on the BRAS according to the authentication and accounting requirements for dialup users. For details about the configuration, see the configuration guide.
- The ONU has been added to the OLT. For details, see **10.6.1.3 Adding an ONU to an OLT**.
- A VDSL2 port has been activated. For details, see **10.6.1.4 Configuring a VDSL2 User Port**.
- The VLAN of the LAN switch port connected to the OLT is consistent with the upstream VLAN of the OLT.
- Residential users generally access the Internet through PPPoE dialup. PPPoE dialup can be performed on PCs or HGWs.
- The configuration processes on HGWs of different models or in different appearances are similar. This section describes how to configure the Internet access service on an HG239 that is connected to an ONU upstream through a LAN.

Copyright © Huawei Technologies Co., Ltd.

Data Plan

Item	Data
ONU line profile	Profile name: fttd T-CONT ID: 4 GEM port ID for Internet access service: 14
Network topology data	Uplink port: 0/19/0 PON port: 0/1/0 ONU IDs: 1 ID of the port on the HGW that is connected to the PC: 1
VLAN Plan	Double-tagged VLAN: ● S-VLAN ID: 100 ● S-VLAN type: smart ● S-VLAN attribute: stacking ● C-VLAN ID: 1001-1002 ● U-VLAN ID: 45 VLAN translation policy: ● ONU: transparently transmits the user VLAN tags carried in the upstream packets sent from the HGW. ● OLT: translates the user VLAN tags to S-VLAN+C-VLAN tags.

Procedure

- Configure the OLT.
  1. Configure a traffic profile.

     Configure traffic profile 8. Set the CIR to off (unlimited), priority to 4, and priority-based scheduling policy to local-setting (that is, queues are scheduled based on the priority specified in the profile).

     NOTE

     Run the **display traffic table ip** command to query the existing traffic profiles in the system. If the existing traffic profiles in the system do not meet the requirements, run the **traffic table ip** command to add a traffic profile.

     ```
     huawei(config)#traffic table ip index 8 name fttd_hsi cir off priority 4 priority-policy local-setting
     ```

  2. Configure the mapping between a GEM port and a VLAN.

     The service flow of user-side VLAN 45 is mapped to GEM port 14 in the ONU line profile.

     NOTE

     Here, the user-side VLAN is the VLAN carried by packets sent from HGW to ONU, namely, U-VLAN.

Copyright © Huawei Technologies Co., Ltd.

```
huawei(config)#ont-lineprofile gpon profile-name fttd
huawei(config-gpon-lineprofile-1)#gem mapping 14 0 vlan 45
huawei(config-gpon-lineprofile-1)#commit
huawei(config-gpon-lineprofile-1)#quit
```

3. Configure the VLAN of the Ethernet port on the ONU.

   Add Ethernet port 1 to VLAN 45 in the ONU service profile.

```
huawei(config)#ont-srvprofile gpon profile-name fttd
huawei(config-gpon-srvprofile-1)#port vlan eth 1 45
huawei(config-gpon-srvprofile-1)#commit
```

4. Create an Internet access service VLAN and add an uplink port to it.

   Add uplink port 0/19/0 to VLAN 100.

```
huawei(config)#vlan 100 smart
huawei(config)#vlan attrib 100 stacking
huawei(config)#port vlan 100 0/19 0
```

5. Create Internet access service flows.

   Set S-VLAN ID to 100 and GEM port ID to 14. Use traffic profile fttd_hsi.

```
huawei(config)#service-port vlan 100 gpon 0/1/0 ont 1 gemport 14 multi-
service
user-vlan 45 tag-transform translate-and-add inner-vlan 1001 inbound
traffic-table
 name fttd_hsi outbound traffic-table name fttd_hsi
```

6. Save the data.

```
huawei(config)#save
```

- Configure the HGW.

1. Log in to the web configuration window.

   a. Enter http://192.168.1.1/cu.html (default IP address) to the address bar of the IE browser and press **Enter**.

   b. In the login dialog box, enter the user name and password of the administrator (the Internet service provider (ISP) provides the default user name and default password). Then, click **OK**.

2. Set parameters for the Internet access service.

   Assume that ports LAN1 and LAN2 are Internet access ports for PCs.

   a. Choose **Network** > **Bandwidth Configuration** from the navigation tree.

   b. Create WAN connection 1 and set parameters based on the following table.

Parameter	Value
Bearing service	INTERNET
VLAN enabling	Enabled: Upstream packets contain VLAN tags. Disabled: Upstream packets do not contain VLAN tags. **NOTE** If **uservlan** is set to **untagged** when you configure a service flow for the Internet access service on the OLT, set this parameter to **Disabled**; otherwise, set it to **Enabled**.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Value
VLANID [1-4094]	If **VLAN enabling** is set to **Enabled**, this parameter takes the value of **uservlan** that is specified when you configure a service flow for the Internet access service on the OLT.
Binding item	LAN1 and LAN2: PCs connected to ports LAN1 and LAN2 can simultaneously access the Internet.
Mode	Bridge: PCs access the Internet through PPPoE dialup.

c. Click **OK**.

3. Restart the HGW.

   Choose **Management** > **Device Management** and click **Restarting the Device**.

----End

10.6.1.6 Configuring the H.248-based Voice Service (Through the CLI)

An optical line terminal (OLT) manages optical network units (ONUs) and applies VoIP configurations to the ONU using the optical network terminal management and control interface (OMCI) protocol. This section describes how to configure the H.248-based voice service.

Prerequisite

- The interface data and PSTN user data corresponding to the MG interface have been configured on the MGC.
- The OLT has been connected to the MGC. The OLT can ping the IP address of the MGC server successfully.
- The ONU has been added to the OLT. For details, see **10.6.1.3 Adding an ONU to an OLT**.
- Different voice services require different ONU software versions. Before the configuration, ensure that the current ONU software version supports H.248. For details, see relevant ONU manuals.

Data Plan

Item	Data
ONU line profile	Profile name: fttd T-CONT ID: 4 GEM port ID: 12

Copyright © Huawei Technologies Co., Ltd.

Item	Data
VLAN plan	Single VLAN tag: ● VLAN ID: 300 ● VLAN type: smart ● VLAN attribute: common ● CVLAN=SVLAN VLAN translation policy: ● ONU: provides the VoIP service and uses the same SVLAN.
Voice parameter	IP address of the MGC server: 200.200.200.200/24 Port ID of the MGC server: 2944

Procedure

Step 1 Configure a traffic profile.

Run the **display traffic table ip** command to query the existing traffic profiles in the system. If the existing traffic profiles in the system do not meet the requirements, run the **traffic table ip** command to add a traffic profile.

Step 2 Configure the mapping between a GEM port and a VLAN.

The service flow of user VLAN 300 is mapped to GEM port 12 in the ONU line profile.

```
huawei(config)#ont-lineprofile gpon profile-name fttd
huawei(config-gpon-lineprofile-1)#gem mapping 12 2 vlan 300
huawei(config-gpon-lineprofile-1)#commit
huawei(config-gpon-lineprofile-1)#quit
```

Step 3 Create a service VLAN and add an uplink port to it.

Add uplink port 0/19/0 to VLAN 300.

```
huawei(config)#vlan 300 smart
huawei(config)#port vlan 300 0/19 0
```

Step 4 Create service flows.

Set the service VLAN to 300, GEM port ID to 12, and user VLAN to 300, and use traffic profile **fttd_voip**.

```
huawei(config)#service-port vlan 300 gpon 0/1/0 ont 1 gemport 12 multi-service
 user-vlan 300 inbound traffic-table name fttd_voip outbound traffic-table name
fttd_voip
huawei(config)#service-port vlan 300 gpon 0/1/0 ont 2 gemport 12 multi-service
 user-vlan 300 inbound traffic-table name fttd_voip outbound traffic-table name
fttd_voip
```

Step 5 Enable the ARP proxy function.

Voice media streams for different users of the same SVLAN fail to interchange because the service ports of the smart VLAN are isolated from each other. Therefore, the ARP proxy function needs to be enabled on the OLT.

Copyright © Huawei Technologies Co., Ltd.

```
huawei(config)#arp proxy enable
huawei(config)#interface vlanif 300
huawei(config-if-vlanif300)#arp proxy enable
huawei(config-if-vlanif300)#quit
```

Step 6 Configure ONU voice service profiles.

ONU voice service profiles include the interface common profile, MGC interface profile, and POTS port profile.

- Interface common profile: saves common attributes of an ONU voice interface, including the fax mode, fax/modem negotiation mode, and priority of the coding and decoding mode.
- MGC interface profile: saves the IP address or domain name of the MGC, protocol port ID of the MGC transport layer to which the MG interface belongs, and DSCP priority of media packets.
- POTS port profile: saves physical attributes of a POTS port on an ONU, including the impedance, transmitting gain, receiving gain, and signaling type of the POTS port.

1. Configure an interface common profile.

   Run the **display ont-mg-attribute-profile** command to query the existing interface common profile in the system. If the existing interface common profile in the system does not meet the requirements, run the **ont-mg-attribute-profile add** command to add an interface common profile.

   In this example, the default interface common profile, namely interface common profile 1 is used.

2. Configure an MGC interface profile.

   Run the **display ont-mgc-profile** command to query the existing MGC interface profile in the system. If the existing MGC interface profile in the system does not meet the requirements, run the **ont-mgc-profile add** command to add an MGC interface profile.

   Create MGC interface profile 2, set the IP address of the MGC to 200.200.200.200, and use default values for other parameters.

   ```
   huawei(config)#ont-mgc-profile add profile-id 2 primary-mgc 200.200.200.200
   ```

3. Configure a POTS port profile.

   Run the **display ont-pots-profile** command to query the existing POTS port profile in the system. If the existing POTS port profile in the system does not meet the requirements, run the **ont-pots-profile add** command to add a POTS port profile.

   In this example, the default POTS port profile, namely POTS port profile 1 is used.

Step 7 Configure the IP addresses of ONU SIP users.

For ONU 1, configure the IP address obtaining mode to the static mode, set the IP addresses to 10.10.10.10/24, set the management VLAN to VLAN 20, and use default values for other parameters.

```
huawei(config)#interface gpon 0/1
huawei(config-if-gpon-0/1)#ont ipconfig 0 1 dhcp vlan 20
```

Step 8 Configure H.248 POTS users.

1. Add an H.248 interface and apply an MGC interface profile to the interface.

   For ONU 1, set the MG ID to 1, apply MGC interface profile 2 to ONU 1, and use default values for other parameters.

   If parameters of an MGC interface profile are changed, the MGC interface profile must be reapplied to the ONU so that the changed parameters can take effect.

Copyright © Huawei Technologies Co., Ltd.

```
huawei(config-if-gpon-0/1)#if-h248 add 0 1 1 mgc-profile profile-id 2
```

2. Add POTS users.

   Add POTS users 1 and 2 to ONU 1, set the MG ID to 1 (identical to the MG ID of the H.248 interface), and set the physical terminal port ID to A0 and A1.

```
huawei(config-if-gpon-0/1)#mgpstnuser add 0 1 1 mgid 1 terminalid A0
huawei(config-if-gpon-0/1)#mgpstnuser add 0 1 2 mgid 1 terminalid A1
```

   Run the **display mgpstnuser attribute** command to check whether the configuration of the POTS user is properly set.

```
huawei(config-if-gpon-0/1)#display mgpstnuser attribute 0 1 1

--------------------------------------------------------------------------------
  F/S/P                       : 0/1/0
  ONT ID                      : 1
  Port ID                     : 1

  MG ID                       : 1
  Terminal ID                 : A0
...//The rest of the response information is omitted.

huawei(config-if-gpon-0/1)#display mgpstnuser attribute 0 2 1

--------------------------------------------------------------------------------
  F/S/P                       : 0/1/0
  ONT ID                      : 1
  Port ID                     : 2

  MG ID                       : 1
  Terminal ID                 : A1
...//The rest of the response information is omitted.
```

Step 9 Apply ONU voice service profiles

After ONU voice service profiles are applied, if parameters in those profiles are changed, those profiles must be reapplied so that the changed parameters can take effect.

1. Apply an interface common profile.

   Run the **if-h248 attribute** command to apply an interface common profile to an H.248 interface or configure the interface customized parameters, or run the **ont-if-h248 bat-apply** command to bulk apply the interface common profiles to H.248 interfaces. If you use these two commands to apply the interface common profiles or configure the interface customized parameters repeatedly, the last configurations take effect.

   In this example, the default interface common profile, namely interface common profile 1 is used.

2. Apply a POTS port profile.

   Run the **pstnport electric** command to apply a POTS port profile to an H.248 interface or configure the interface customized parameters, or run the **ont-pstnport electric bat-apply** command to bulk apply the POTS port profiles to H.248 interfaces. If you use these two commands to apply the POTS port profiles or configure the interface customized parameters repeatedly, the last configurations take effect.

   In this example, the default POTS port profile, namely POTS port profile 1 is used.

Step 10 (Optional) Configure the H.248 user codec.

Run the **mgpstnuser codec** command to configure the H.248 user codec. The H.248 user codec will not be configured independently in this example.

Step 11 Save the data.

Copyright © Huawei Technologies Co., Ltd.

```
huawei(config)#save
```

----End

10.6.1.7 Configuring the H.248-based Voice Service (on a Web Page)

The OLT is connected to the remote ONU through a GPON port to provide users with the IP-based high-quality and low-cost VoIP service.

Prerequisite

- The interface data and PSTN user data corresponding to the MG interface have been configured on the MGC.
- The OLT has been connected to the MGC. The OLT can ping the IP address of the MGC server successfully.
- The ONU has been added to the OLT. For details, see **10.6.1.3 Adding an ONU to an OLT**.
- Different voice services require different ONU software versions. Before the configuration, ensure that the current ONU software version supports H.248. For details, see relevant ONU manuals.

Data Plan

Item	Data
ONU line profile	Profile name: fttd T-CONT ID: 4 GEM port ID: 12
VLAN plan	Single VLAN tag: ● VLAN ID: 300 ● VLAN type: smart ● VLAN attribute: common ● CVLAN=SVLAN VLAN translation policy: ● ONU: provides the VoIP service and uses the same SVLAN.
Voice parameter	IP address of the MGC server: 200.200.200.200/24 Port ID of the MGC server: 2944

Procedure

- Configure the OLT.
  1. Configure a traffic profile.

Copyright © Huawei Technologies Co., Ltd.

Run the **display traffic table ip** command to query the existing traffic profiles in the system. If the existing traffic profiles in the system do not meet the requirements, run the **traffic table ip** command to add a traffic profile.

Set the profile name to **fttd_voip** and do not limit the upstream and downstream rates. Set the priority to **5** and packets are scheduled according to the priority carried.

```
huawei(config)#traffic table ip name fttd_voip cir off priority 5 priority-
policy
 local-setting
```

2. Configure the mapping between a GEM port and a VLAN.

   The service flow of user VLAN 300 is mapped to GEM port 12 in the ONU line profile.

```
huawei(config)#ont-lineprofile gpon profile-name fttd
huawei(config-gpon-lineprofile-1)#gem mapping 12 2 vlan 300
huawei(config-gpon-lineprofile-1)#commit
huawei(config-gpon-lineprofile-1)#quit
```

3. Create a service VLAN and add an uplink port to it.

   Add uplink port 0/19/0 to VLAN 300.

```
huawei(config)#vlan 300 smart
huawei(config)#port vlan 300 0/19 0
```

4. Create service flows.

   Set the service VLAN to 300, GEM port ID to 12, and user VLAN to 300, and use traffic profile **fttd_voip**.

```
huawei(config)#service-port vlan 300 gpon 0/1/0 ont 1 gemport 12 multi-
service
 user-vlan 300 inbound traffic-table name fttd_voip outbound traffic-table
name
fttd_voip
huawei(config)#service-port vlan 300 gpon 0/1/0 ont 2 gemport 12 multi-
service
 user-vlan 300 inbound traffic-table name fttd_voip outbound traffic-table
name
fttd_voip
```

5. Enable the ARP proxy function.

   Voice media streams for different users of the same SVLAN fail to interchange because the service ports of the smart VLAN are isolated from each other. Therefore, the ARP proxy function needs to be enabled on the OLT.

```
huawei(config)#arp proxy enable
huawei(config)#interface vlanif 300
huawei(config-if-vlanif300)#arp proxy enable
huawei(config-if-vlanif300)#quit
```

6. Save the data.

```
huawei(config)#save
```

- Configure the ONU on the Web page.

  Log in to the web configuration window.

  1. Configure the IP address of the PC network adapter to be in the same network segment with the IP address of the local maintenance Ethernet port on the ONU (default: 192.168.100.1).
  2. Open the Web browser, and enter the IP address of the local maintenance Ethernet port on the ONU. In the login window, enter the user name (default: telecomadmin)

Copyright © Huawei Technologies Co., Ltd.

and password (default: admintelecom) of the administrator. After the password is authenticated, the Web configuration window is displayed.

NOTE

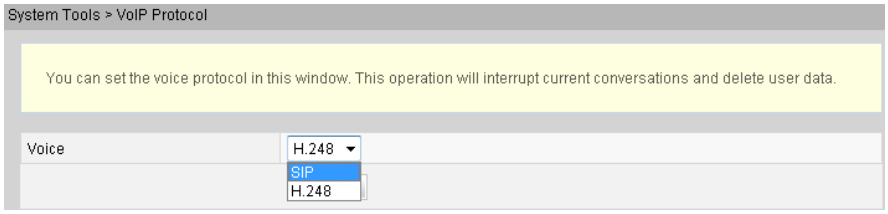
The webpage login supports SSL3.0, TLS1.0, and TLS1.1. It is recommended that you use high-security TLS1.1 if you log in to the ONU using https.

1. Configure the voice protocol.

   NOTE

   The default voice protocol is SIP. Before the configuration, perform this step to change the voice protocol.

   1. Choose **System Tools** > **VoIP Protocol** from the main menu.
   2. In the pane on the right side of the window, set **voice** to **H.248**.
   3. Click . The configuration takes effect.



2. Configure parameters for the voice WAN interface.

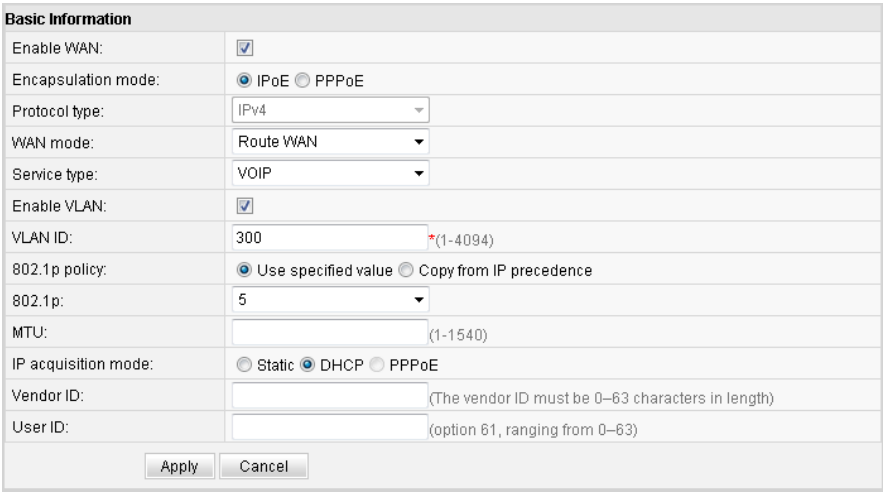
   a. Choose **WAN** > **WAN Configuration**.

   b. In the right pane, click **New**. In the dialog box that is displayed, set the parameters as follows:

   - Select **Enable WAN Connection** to enable the new WAN connection.
   - Set **Service List** to **VOIP**.
   - Set **Mode** to **Route WAN**.
   - Set **VLAN ID** to **300**.
   - Set **802.1p** to **5**.
   - Set **IP Acquisition Mode** to **DHCP**.

   Figure 10-6 shows the parameter settings.

Figure 10-6 Parameter settings on the Web page for the voice WAN interface



Copyright © Huawei Technologies Co., Ltd.

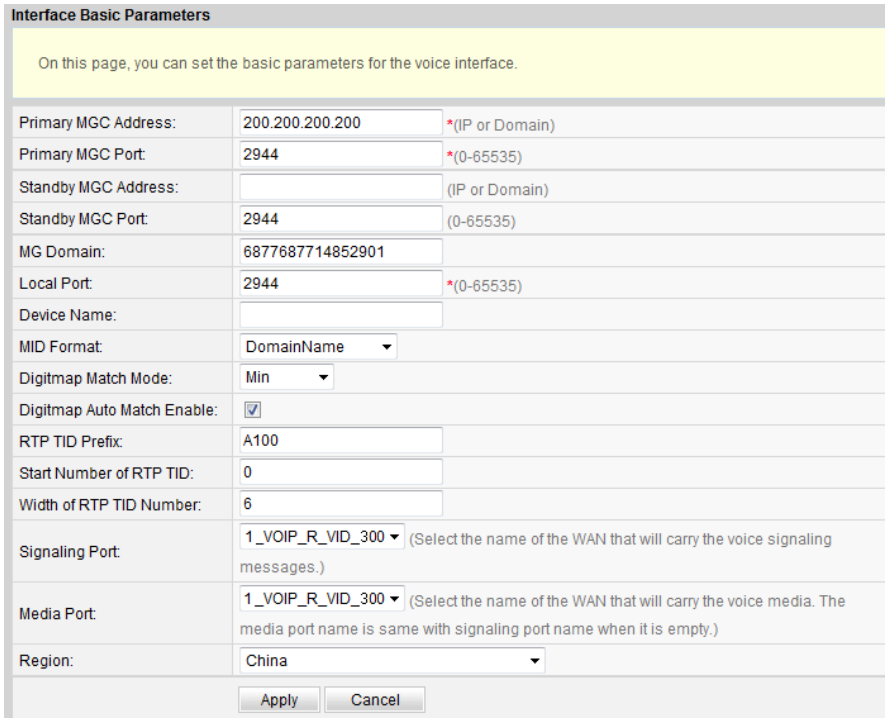
c. Click **Apply**.

3. Configure the parameters of the H.248-based voice interface.
   a. In the navigation tree, choose **Voice** > **VoIP Basic Configuration**.
   b. In the right pane, configure the parameters of the H.248-based voice interface as follows (other parameters use the default settings):
      - Set **MGC Address** below **Primary Server** to **200.200.200.200**.
      - MID Format: DomainName
      - MG Domain: 6877687714852901
      - Signaling Port: 1_VOIP_R_VID_300
      - Region: China

      NOTE

      - The parameters of the H.248-based voice interface must be consistent with the corresponding configuration on the media gateway controller (MGC).
      - If dual-homing is configured, **MGC Address** below **Secondary Server** must be configured.
      - **MID Format** can be set to **Domain Name**, **IP**, or **Device**. If **MID Format** is set to **Domain Name** or **Device**, the setting must be consistent with the corresponding configuration on the MGC.
      - **Domain Name** is ONU's domain name registered with the MGC. It is globally unique. **Domain Name** in this example is ONU's SN.
      - If **Media Port** is empty, the parameter value is the same as **Signaling Port**. The media streams are not isolated from signaling streams. If the upper-layer network requires isolation of media streams from signaling streams, create different traffic streams for the media streams and signaling streams on the OLT, create different WAN ports on the ONU, and bind the created WAN ports to **Media Port** and **Signaling Port**.
      - **Profile Index** can be set to **Default**, **BT**, **FT**, **KPN**, **PCCW**, **ZTE**, or **BELL**. Choose the value based on the MGC type. **Profile Index** is set to **Default** (indicating interconnection with Huawei MGC) in this example. If the settings do not meet requirements, configure **UserDefine**. For details about how to configure this parameter, contact Huawei technical support engineers.
      - When the ONU is interconnected with a third-party softswitch, check **RTP TID Prefix**, **Start Number of RTP TID**, and **Width of RTP TID Number**.

Copyright © Huawei Technologies Co., Ltd.



c. Click . The configuration takes effect.

4. Configure parameters of the H.248-based voice users.

a. In the navigation tree, choose **Voice** > **VoIP Basic Configuration**.

b. In the right pane, configure the parameters of voice user 1 as follows:

- Line Name: A0
- Associated POTS: 1 (binding port TEL1 on the ONU)
- Select **Enable Line Name** to enable the voice user configuration.

c. Click . The configuration takes effect.

d. In the right pane, click **New** to add voice user 2, and configure the parameters of voice user 2 as follows:

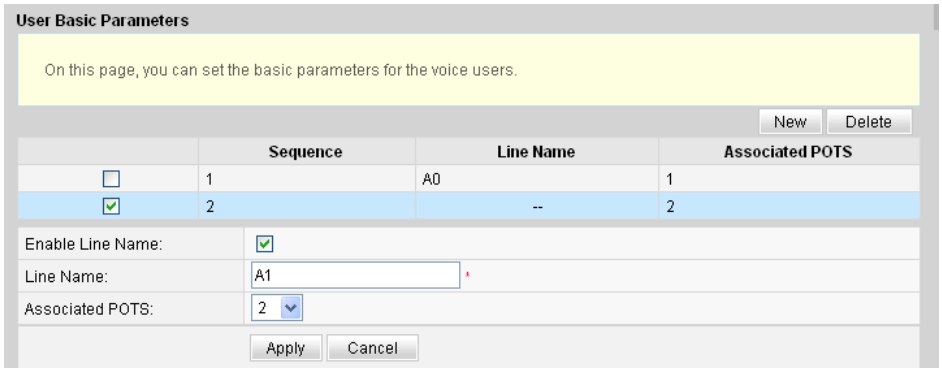
- Line Name: A1
- Associated POTS: 2 (binding port TEL2 on the ONU)
- Select **Enable Line Name** to enable the voice user configuration.

e. Click . The configuration takes effect.

NOTE

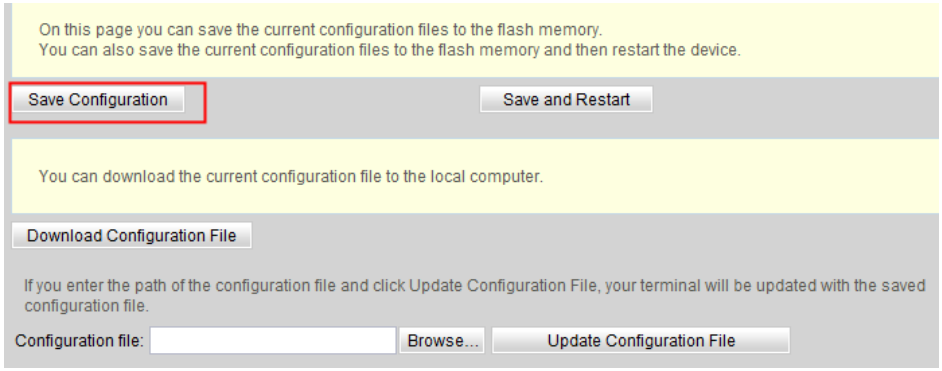
- The terminal IDs **A0** and **A1** must be consistent with the corresponding configuration on the MGC.
- If **Associated POTS** is **1**, port TEL1 on the ONU is bound. If **Associated POTS** is **2**, port TEL2 on the ONU is bound.

Copyright © Huawei Technologies Co., Ltd.



5. Save the configuration.

   In the navigation tree, choose **System Tools** > **Configuration File**. In the right pane, click **Save Configuration** to save the configuration.



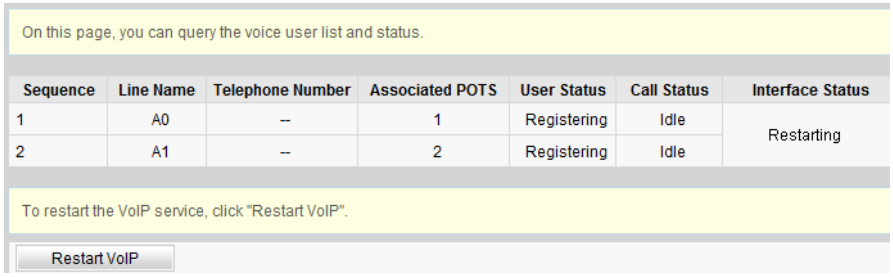
6. Restart the voice service and check the voice user status.

   a. Choose **Status** > **VoIP Information**. In the right pane, click **Restart VoIP**.

   b. Choose **Status** > **VoIP Information**. In the right pane, **User Status** is **Up**.

   Figure 10-7 shows the user status.

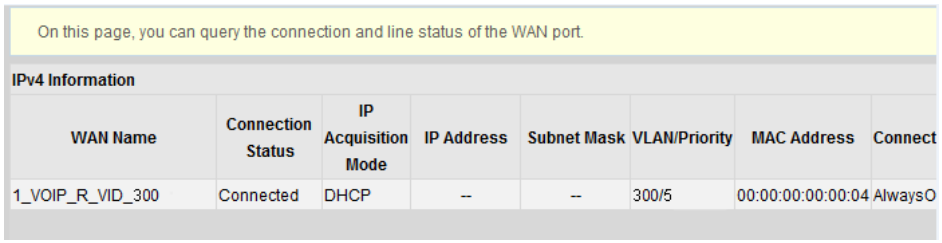
   Figure 10-7 Registration status of voice users



7. Check the ONU connection status.

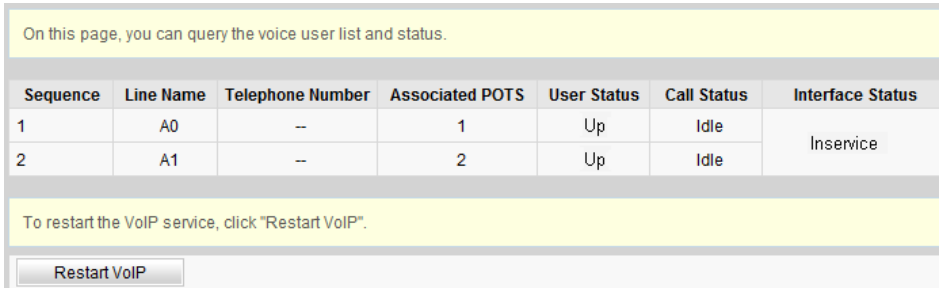
   In the navigation tree, choose **Status** > **WAN Information**. In the right pane, **Status** is **Connected** and the obtained IP address is displayed at **IP Address**.

Copyright © Huawei Technologies Co., Ltd.



8. Check the registration status of a voice user.

   In the navigation tree, choose **Status** > **VoIP Information**. In the right pane, **User Status** is **Up**.



----End

10.6.1.8 Configuring the SIP-based Voice Service (Through the CLI)

The OLT manages ONUs and applies VoIP configurations to the ONU using the OMCI protocol. This topic describes how to configure the SIP-based voice service.

Prerequisites

- The SIP interface data and POTS user data corresponding to the MG interface have been configured on the SIP server.
- The connection between the OLT and the SIP server is set up. The OLT can ping the IP address of the SIP server successfully.
- The ONU has been added to the OLT. For details, see **10.6.1.3 Adding an ONU to an OLT**.
- Different voice services require different ONU software versions. Before the configuration, ensure that the current ONU software version supports SIP. For details, see relevant ONU manuals.

Data Plan

Item	Data
ONU line profile	Profile name: ftth T-CONT ID: 4 GEM port ID: 12

Copyright © Huawei Technologies Co., Ltd.

Item	Data
VLAN plan	Single VLAN tag: ● VLAN ID: 300 ● VLAN type: smart ● VLAN attribute: common ● CVLAN=SVLAN VLAN translation policy: ● ONU: provides the VoIP service and uses the same SVLAN.
Voice parameter	IP address of the SIP server: 200.200.200.200/24 Port ID of the SIP server: 5060 Home domain name: huawei.com User phone number 1: 77730010 User phone number 2: 77730020

Procedure

Step 1 Configure a traffic profile.

Run the **display traffic table ip** command to query the existing traffic profiles in the system. If the existing traffic profiles in the system do not meet the requirements, run the **traffic table ip** command to add a traffic profile.

Step 2 Configure the mapping between a GEM port and a VLAN.

The service flow of user VLAN 300 is mapped to GEM port 12 in the ONU line profile.

```
huawei(config)#ont-lineprofile gpon profile-name fttd
huawei(config-gpon-lineprofile-1)#gem mapping 12 2 vlan 300
huawei(config-gpon-lineprofile-1)#commit
huawei(config-gpon-lineprofile-1)#quit
```

Step 3 Create a service VLAN and add an uplink port to it.

Add uplink port 0/19/0 to VLAN 300.

```
huawei(config)#vlan 300 smart
huawei(config)#port vlan 300 0/19 0
```

Step 4 Create service flows.

Set the service VLAN to 300, GEM port ID to 12, and user VLAN to 300, and use traffic profile **fttd_voip**.

```
huawei(config)#service-port vlan 300 gpon 0/1/0 ont 1 gemport 12 multi-service
 user-vlan 300 inbound traffic-table name fttd_voip outbound traffic-table name
fttd_voip
huawei(config)#service-port vlan 300 gpon 0/1/0 ont 2 gemport 12 multi-service
 user-vlan 300 inbound traffic-table name fttd_voip outbound traffic-table name
fttd_voip
```


Copyright © Huawei Technologies Co., Ltd.

Step 5 Configure ONU voice service profiles.

ONU voice service profiles include the interface common profile, SIP agent profile, SIP service data profile, POTS port profile, and digitmap profile.

- Interface common profile: saves common attributes of an ONU voice interface, including the fax mode, fax/modem negotiation mode, and priority of the coding and decoding mode.
- SIP agent profile: saves the SIP agent information about an ONU, including the IP address and domain name of the SIP agent server and attributes of media packets and signaling packets.
- SIP service data profile: saves the data information about ONU voice services, including the rights of the call waiting service, three-party service, call forwarding service, and call holding service.
- POTS port profile: saves physical attributes of a POTS port on an ONU, including the impedance, transmitting gain, receiving gain, and signaling type of the POTS port.
- Digitmap profile: saves the digitmap information about an ONU, including the timeout time of the digitmap timer and the digitmap format.

1. Configure an interface common profile.

   Run the **display ont-mg-attribute-profile** command to query the existing interface common profile in the system. If the existing interface common profile in the system does not meet the requirements, run the **ont-mg-attribute-profile add** command to add an interface common profile.

   In this example, the default interface common profile, namely interface common profile 1 is used.

2. Configure an SIP agent profile.

   Run the **display ont-sipagent-profile** command to query the existing SIP agent profile in the system. If the existing SIP agent profile in the system does not meet the requirements, run the **ont-sipagent-profile add** command to add an SIP agent profile.

   Create SIP agent profile 2, set the IP address of the SIP server to 200.200.200.200, and use default values for other parameters.

   ```
   huawei(config)#ont-sipagent-profile add profile-id 2 proxy-server
   200.200.200.200
   ```

3. Configure an SIP service data profile.

   Run the **display ont-siprightflag-profile** command to query the existing SIP agent profile in the system. If the existing SIP service data profile in the system does not meet the requirements, run the **ont-siprightflag-profile add** command to add an SIP service data profile.

   In this example, the default SIP service data profile, namely SIP service data profile 1 is used.

4. Configure a POTS port profile.

   Run the **display ont-pots-profile** command to query the existing POTS port profile in the system. If the existing POTS port profile in the system does not meet the requirements, run the **ont-pots-profile add** command to add a POTS port profile.

   In this example, the default POTS port profile, namely POTS port profile 1 is used.

5. Configure a digitmap profile.

   Run the **display ont-digitmap-profile** command to query the existing digitmap profile in the system. If the existing digitmap profile in the system does not meet the requirements, run the **ont-digitmap-profile add** command to add a digitmap profile.

Copyright © Huawei Technologies Co., Ltd.

In this example, the default digitmap profile, namely digitmap profile 1 is used.

Step 6 Configure an IP address for an ONU SIP user.

For ONU 1, configure the IP address obtaining mode to the DHCP mode, set the management VLAN to VLAN 20, and use default values for other parameters.

```
huawei(config)#interface gpon 0/1
huawei(config-if-gpon-0/1)#ont ipconfig 0 1 dhcp vlan 20
```

Step 7 Configure SIP POTS users.

1. Add an SIP interface and apply an SIP agent profile to the interface.

   For ONU 1, set the MG ID to 1, apply SIP agent profile 2 to ONU 1, and use default values for other parameters.

   If parameters in an SIP agent profile are changed, the SIP agent profile must be reapplied to the ONU so that the changed parameters can take effect.

   ```
   huawei(config-if-gpon-0/1)#if-sip add 0 1 1 sipagent-profile profile-id 2
   ```

2. Add POTS users.

   For ONU 1, set the MG ID to 1 (identical to the MG ID of the added SIP interface), create two POTS users named huawei1, set passwords to user1 and user2, set their phone numbers to 77730010 and 77730020 and use default values for other parameters.

   ```
   huawei(config-if-gpon-0/1)#sippstnuser add 0 1 1 mgid 1 username huawei1 telno
   77730010
   huawei(config-if-gpon-0/1)#sippstnuser add 0 2 1 mgid 1 username huawei2 telno
   77730020
   ```

   Run the **display sippstnuser attribute** command to check whether the configuration of the POTS user is properly set.

   ```
   huawei(config-if-gpon-0/1)#display sippstnuser attribute 0 1 1

   ------------------------------------------------------------------------------
     F/S/P                       : 0/1/0
     ONT ID                      : 1
     Port ID                     : 1

     MG ID                       : 1
     Telephone NO.               : 77730010
     User name                   : huawei1
     Password                    : user1
   ...//The rest of the response information is omitted.

   huawei(config-if-gpon-0/1)#display sippstnuser attribute 0 1 2

   ------------------------------------------------------------------------------
     F/S/P                       : 0/1/0
     ONT ID                      : 1
     Port ID                     : 2

     MG ID                       : 1
     Telephone NO.               : 77730020
     User name                   : huawei2
     Password                    : user2
   ...//The rest of the response information is omitted.
   ```

Step 8 Apply and bind an ONU voice service profile to an SIP interface

Currently, the interface common profile, SIP agent profile, SIP service data profile, and POTS port profile can be applied to an SIP interface, and the digitmap profile can be bound to an SIP interface.

Copyright © Huawei Technologies Co., Ltd.

For profiles that can be applied to an SIP interface, if parameters in those profiles are changed, those profiles must be reapplied to the SIP interface so that the changed parameters can take effect. For profiles that can be bound to an SIP interface, if parameters in those profiles are changed, those profiles do not need to be rebound to the SIP interface and the changed parameters can take effect.

The method for applying an SIP agent profile is introduced in step **Step 7.1**. The following will introduce the methods for applying an interface common profile, an SIP service data profile, and a POTS port profile, and the method for binding a digitmap to an SIP interface.

1. Apply an interface common profile.

   Run the **if-sip attribute** command to apply an interface common profile to an SIP interface or configure the interface customized parameters, or run the **ont-if-sip bat-apply from** command to bulk apply the interface common profiles to SIP interfaces. If you use these two commands to apply the interface common profiles or configure the interface customized parameters repeatedly, the last configurations take effect.

   In this example, the default interface common profile, namely interface common profile 1 is used.

2. Apply an SIP service data profile.

   Run the **sippstnuser rightflag** command to apply an SIP service data profile to an SIP interface or configure the interface customized parameters, or run the **ont-sippstnuser bat-apply from** command to bulk apply the SIP service data profiles to SIP interfaces. If you use these two commands to apply the SIP service data profiles or configure the interface customized parameters repeatedly, the last configurations take effect.

   In this example, the default SIP service data profile, namely SIP service data profile 1 is used.

3. Apply a POTS port profile.

   Run the **pstnport electric** command to apply a POTS port profile to an SIP interface or configure the interface customized parameters, or run the **ont-pstnport electric bat-apply** command to bulk apply the POTS port profiles to SIP interfaces. If you use these two commands to apply the POTS port profiles or configure the interface customized parameters repeatedly, the last configurations take effect.

   In this example, the default POTS port profile, namely POTS port profile 1 is used.

4. Bind a digitmap profile.

   Run the **sippstnuser digitmap** command to bind a digitmap profile to an SIP interface, or run the **ont-sippstnuser bat-bind from** command to bulk apply the digitmap profiles to SIP interfaces. If you use these two commands to bind the SIP service data profiles to SIP ports repeatedly, the last configurations take effect.

   In this example, the default digitmap profile, namely digitmap profile 1 is used.

Step 9 (Optional) Configure the SIP user codec.

Run the **sippstnuser codec** command to configure the SIP user codec. The SIP user codec will not be configured independently in this example.

Step 10 Save the data.

```
huawei(config)#save
```

----End

Copyright © Huawei Technologies Co., Ltd.

10.6.1.9 Configuring the SIP-based Voice Service (on a Web Page)

The OLT is connected to the remote ONU through a GPON port to provide users with the SIP-based high-quality and low-cost VoIP service.

Prerequisites

- The SIP interface data and POTS user data corresponding to the MG interface have been configured on the SIP server.
- The connection between the OLT and the SIP server is set up. The OLT can ping the IP address of the SIP server successfully.
- The ONU has been added to the OLT. For details, see **10.6.1.3 Adding an ONU to an OLT**.
- Different voice services require different ONU software versions. Before the configuration, ensure that the current ONU software version supports SIP. For details, see relevant ONU manuals.

Data Plan

Item	Data
ONU line profile	Profile name: ftth T-CONT ID: 4 GEM port ID: 12
VLAN plan	Single VLAN tag: ● VLAN ID: 300 ● VLAN type: smart ● VLAN attribute: common ● CVLAN=SVLAN VLAN translation policy: ● ONU: provides the VoIP service and uses the same SVLAN.
Voice parameter	IP address of the SIP server: 200.200.200.200/24 Port ID of the SIP server: 5060 Home domain name: huawei.com User phone number 1: 77730010 User phone number 2: 77730020

Procedure

- Configure the OLT.
  1. Configure a traffic profile.

Copyright © Huawei Technologies Co., Ltd.

Run the **display traffic table ip** command to query the existing traffic profiles in the system. If the existing traffic profiles in the system do not meet the requirements, run the **traffic table ip** command to add a traffic profile.

Set the profile name to **fttd_voip** and do not limit the upstream and downstream rates. Set the priority to **5** and packets are scheduled according to the priority carried.

```
huawei(config)#traffic table ip name fttd_voip cir off priority 5 priority-
policy
 local-setting
```

2. Configure the mapping between a GEM port and a VLAN.

   The service flow of user VLAN 300 is mapped to GEM port 12 in the ONU line profile.

```
huawei(config)#ont-lineprofile gpon profile-name fttd
huawei(config-gpon-lineprofile-1)#gem mapping 12 2 vlan 300
huawei(config-gpon-lineprofile-1)#commit
huawei(config-gpon-lineprofile-1)#quit
```

3. Create a service VLAN and add an uplink port to it.

   Add uplink port 0/19/0 to VLAN 300.

```
huawei(config)#vlan 300 smart
huawei(config)#port vlan 300 0/19 0
```

4. Create service flows.

   Set the service VLAN to 300, GEM port ID to 12, and user VLAN to 300, and use traffic profile **fttd_voip**.

```
huawei(config)#service-port vlan 300 gpon 0/1/0 ont 1 gemport 12 multi-
service
 user-vlan 300 inbound traffic-table name fttd_voip outbound traffic-table
name
fttd_voip
huawei(config)#service-port vlan 300 gpon 0/1/0 ont 2 gemport 12 multi-
service
 user-vlan 300 inbound traffic-table name fttd_voip outbound traffic-table
name
fttd_voip
```

5. Enable the ARP proxy function.

   Voice media streams for different users of the same SVLAN fail to interchange because the service ports of the smart VLAN are isolated from each other. Therefore, the ARP proxy function needs to be enabled on the OLT.

```
huawei(config)#arp proxy enable
huawei(config)#interface vlanif 300
huawei(config-if-vlanif300)#arp proxy enable
huawei(config-if-vlanif300)#quit
```

6. Save the data.

```
huawei(config)#save
```

- Configure the ONU on the Web page.

  Log in to the web configuration window.

  1. Configure the IP address of the PC network adapter to be in the same network segment with the IP address of the local maintenance Ethernet port on the ONU (default: 192.168.100.1).
  2. Open the Web browser, and enter the IP address of the local maintenance Ethernet port on the ONU. In the login window, enter the user name (default: telecomadmin)

Copyright © Huawei Technologies Co., Ltd.

and password (default: admintelecom) of the administrator. After the password is authenticated, the Web configuration window is displayed.

NOTE

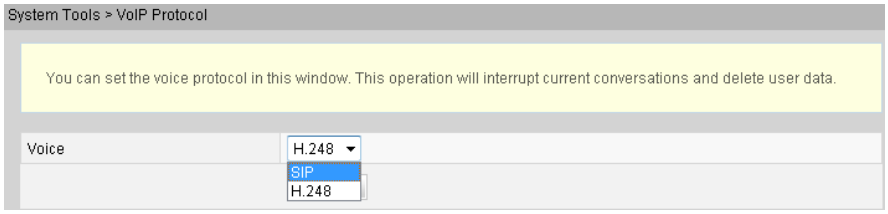
The webpage login supports SSL3.0, TLS1.0, and TLS1.1. It is recommended that you use high-security TLS1.1 if you log in to the ONU using https.

1. Configure the voice protocol.

   NOTE

   The default voice protocol is SIP. Before the configuration, perform this step to change the voice protocol.

   1. Choose **System Tools** > **VoIP Protocol** from the main menu.
   2. In the pane on the right side of the window, set **voice** to **H.248**.
   3. Click . The configuration takes effect.



2. Configure parameters for the voice WAN interface.

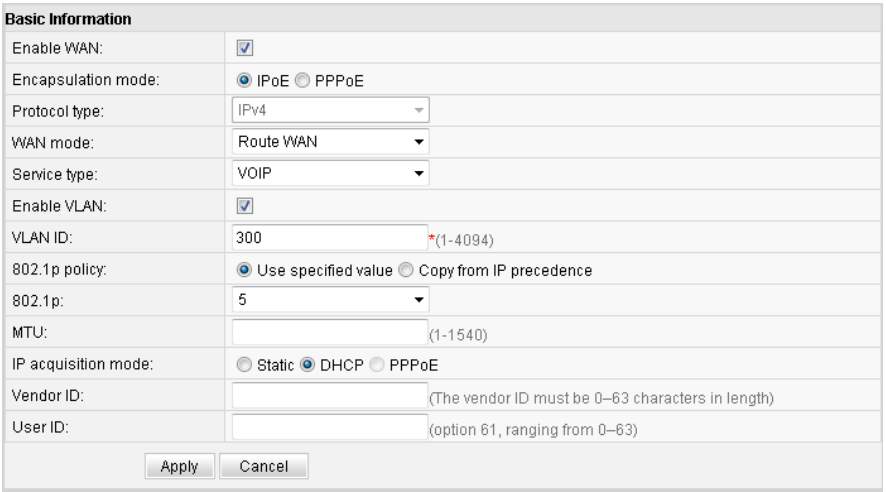
   a. Choose **WAN** > **WAN Configuration**.

   b. In the right pane, click **New**. In the dialog box that is displayed, set the parameters as follows:

   - Select **Enable WAN Connection** to enable the new WAN connection.
   - Set **Service List** to **VOIP**.
   - Set **Mode** to **Route WAN**.
   - Set **VLAN ID** to **300**.
   - Set **802.1p** to **5**.
   - Set **IP Acquisition Mode** to **DHCP**.

   Figure 10-8 shows the parameter settings.

Figure 10-8 Parameter settings on the Web page for the voice WAN interface



Copyright © Huawei Technologies Co., Ltd.

c. Click **Apply**.

3. Configure parameters of the SIP-based voice interface.

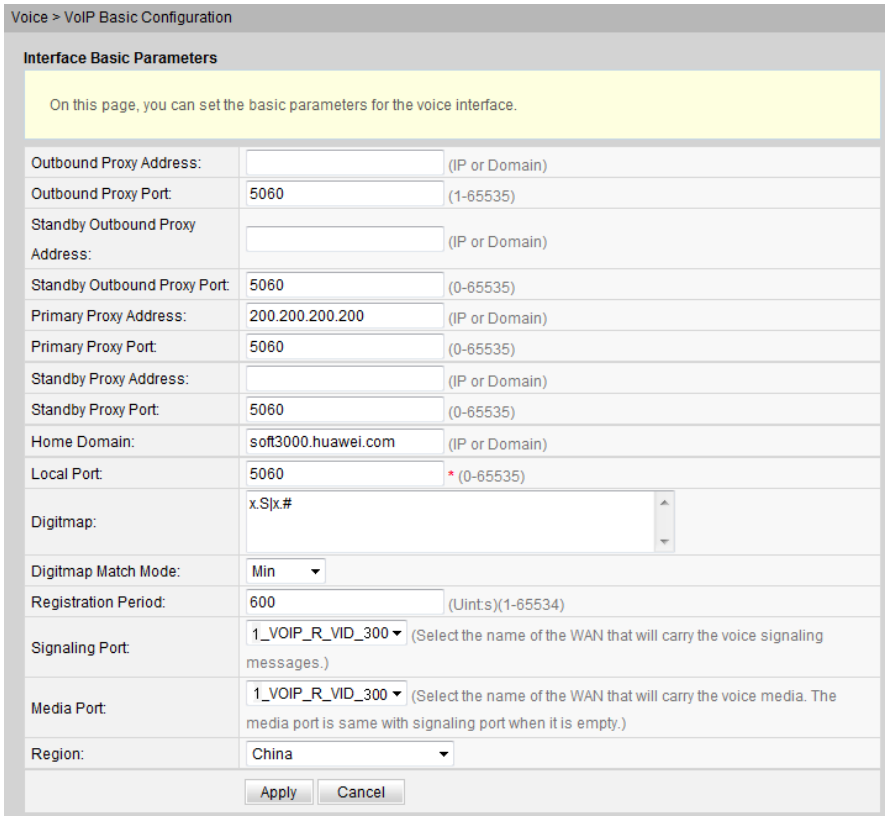
a. In the navigation tree, choose **Voice** > **VoIP Basic Configuration**.

b. In the right pane, configure parameters of the SIP-based voice interface as follows (other parameters use the default settings):

- Set **Proxy Server Address** below **Primary Server** to **200.200.200.200**.
- Home Domain: softx3000.huawei.com
- Signaling Port: 1_VOIP_R_VID_300
- Region: China

NOTE

- The parameters of the SIP-based voice interface must be consistent with the corresponding configuration on the softswitch.
- If dual-homing is configured, **Proxy Server Address** below **Secondary Server** must be configured.
- If **Signaling Port** is empty, the parameter value is the same as **Media Port**. If the upper-layer network requires isolation of media streams from signaling streams, create different traffic streams for the media streams and signaling streams on the OLT, create different WAN ports on the ONU, and bind the created WAN ports to **Media Port** and **Signaling Port**. When the packet is forwarded from two WAN ports, the configured VLAN is carried by default.



c. Click . The configuration takes effect.

4. Configure parameters of the SIP-based voice users.

Copyright © Huawei Technologies Co., Ltd.

a. In the navigation tree, choose **Voice** > **VoIP Basic Configuration**.

b. In the right pane, configure parameters of voice user 1 as follows:

- Register User Name: 80001234
- Auth User Name: 80001234@softx3000.huawei.com
- Password: iadtest1
- Associated POTS: 1 (binding port TEL1 on the ONU)
- Select **Enable** to enable the voice user configuration.

c. Click . The configuration takes effect.

d. Register User Name: 80001235

e. Auth User Name: 80001235@softx3000.huawei.com

f. Password: iadtest2

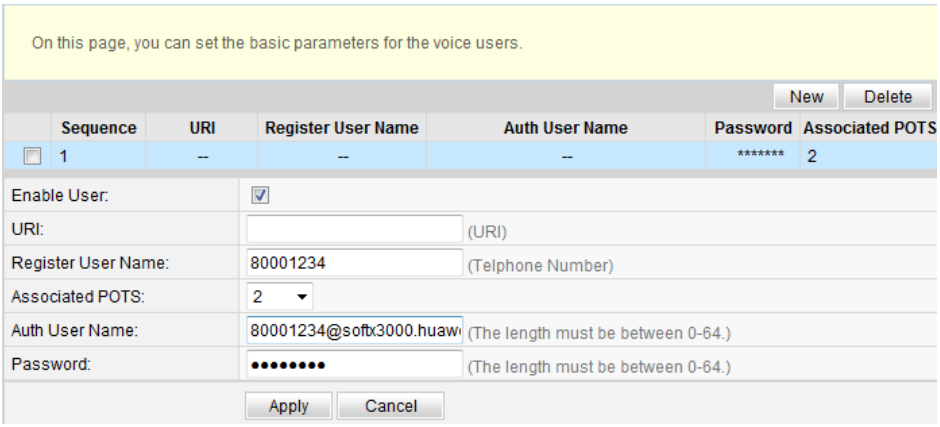
g. Associated POTS: 2 (binding port TEL2 on the ONU)

h. Select **Enable User** to enable the voice user configuration.

i. Click . The configuration takes effect.

NOTE

- The parameters of the SIP-based voice user must be consistent with the corresponding configuration on the softswitch.
- If **Associated POTS** is **1**, port TEL1 on the ONU is bound. If **Associated POTS** is **2**, port TEL2 on the ONU is bound.

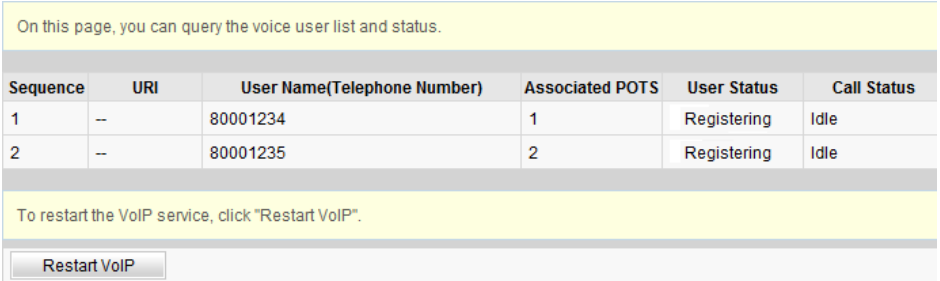


5. Save the data.

```
huawei(config)#save
```

6. Restart the voice process.

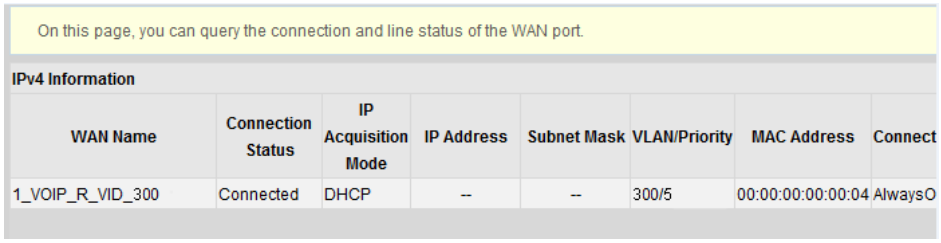
In the navigation tree, choose **Status** > **VoIP Information**. In the right pane, click **Restart VoIP**.



Copyright © Huawei Technologies Co., Ltd.

7. Check the ONU connection status.

   In the navigation tree, choose **Status** > **WAN Information**. In the right pane, **Status** is **Connected** and the obtained IP address is displayed at **IP Address**.

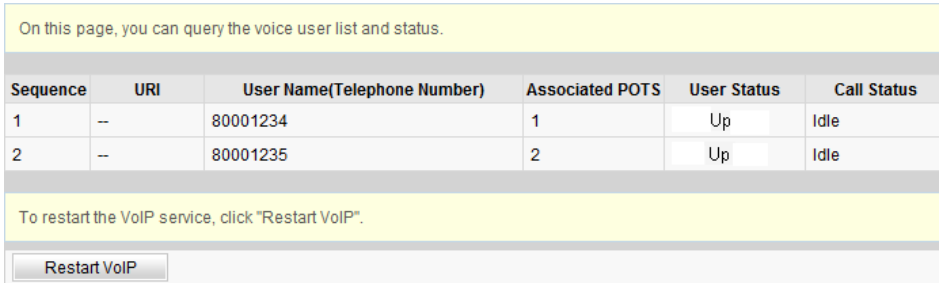

On this page, you can query the connection and line status of the WAN port.

IPv4 Information

WAN Name	Connection Status	IP Acquisition Mode	IP Address	Subnet Mask	VLAN/Priority	MAC Address	Connect
1_VOIP_R_VID_300	Connected	DHCP	--	--	300/5	00:00:00:00:00:04	AlwaysO

8. Check the registration status of the voice user.

   In the navigation tree, choose **Status** > **VoIP Information**. In the right pane, **User Status** is **Up**.


On this page, you can query the voice user list and status.

Sequence	URI	User Name(Telephone Number)	Associated POTS	User Status	Call Status
1	--	80001234	1	Up	Idle
2	--	80001235	2	Up	Idle

To restart the VoIP service, click "Restart VoIP".

Restart VoIP

----End

10.6.1.10 Configuring the BTV Service

The OLT is connected to the remote bridging ONU through a GPON port to provide users with the multicast service.

Prerequisites

- The OLT is connected to the BRAS and the multicast source.
- The VLAN of the LAN switch port connected to the OLT is the same as the upstream VLAN of the OLT.
- The ONU has been added to the OLT. For details, see **10.6.1.3 Adding an ONU to an OLT**.
- A VDSL2 port has been activated. For details, see **10.6.1.4 Configuring a VDSL2 User Port**.

Data Plan

Table 10-4 Data plan

Item	Data
ONU line profile	Profile name: fttd T-CONT ID: 4 GEM port ID: 13

Copyright © Huawei Technologies Co., Ltd.

Item	Data
Traffic profile	ID: 8 802.1p priority: 4 CIR: off (unlimited) Priority-based scheduling policy: local-setting
VLAN Plan	Single VLAN tag: ● SVLAN ID: 1000 ● HGW VLAN: 43 ● MVLAN ID: 1000 ● VLAN type: smart ● VLAN attribute: common VLAN translation policy: ● ONU: translates the user VLAN tags carried in the upstream packets sent from the HGW to MVLAN tags. ● OLT: duplicates multicast packets based on PON ports with MVLAN unchanged.
Multicast service data	Multicast protocol: IGMP proxy Multicast version: IGMPv2 Multicast program: dynamic obtaining mode

Procedure

- Configure the OLT.
  1. Configure a traffic profile.

     Configure traffic profile 8. Set the CIR to off (unlimited), priority to 4, and priority-based scheduling policy to local-setting (that is, queues are scheduled based on the priority specified in the profile).

     NOTE

     Run the **display traffic table ip** command to query the existing traffic profiles in the system. If the existing traffic profiles in the system do not meet the requirements, run the **traffic table ip** command to add a traffic profile.

     ```
     huawei(config)#traffic table ip index 8 cir off priority 4 priority-policy
     local-setting
     ```

  2. Configure the mapping relationship between a GEM port and a VDSL2 port on the ONU.

     In the ONU line profile, the service flow of the VDSL2 port is mapped to GEM port 13.

     ```
     huawei(config)#ont-lineprofile gpon profile-name fttd
     huawei(config-gpon-lineprofile-1)#gem mapping 13 1 vlan 1000
     ```


Copyright © Huawei Technologies Co., Ltd.

```
huawei(config-gpon-lineprofile-1)#commit
huawei(config-gpon-lineprofile-1)#quit
```

3. Configure the VLAN of the VDSL2 port on the ONU.

   If the ONU is connected to the STB through VDSL2 port 2, add Ethernet port 2 to VLAN 1000.

```
huawei(config)#ont-srvprofile gpon profile-name fttd
huawei(config-gpon-srvprofile-1)#port vlan vdsl 1 translation 1000 user-vlan 43
huawei(config-gpon-srvprofile-1)#multicast-forward tag translation 43
huawei(config-gpon-srvprofile-1)#commit
huawei(config-gpon-srvprofile-1)#quit
```

4. Configure the native VLAN of the ONU port.

   If the ONU is connected to the STB through VDSL2 port 1, the native VLAN ID is 1000.

```
huawei(config)#interface gpon 0/1
huawei(config-if-gpon-0/1)#ont port native-vlan 0 1 vdsl 1 vlan 1000
huawei(config-if-gpon-0/1)#quit
```

5. Create a service VLAN and add an uplink port to it.

   Add uplink port 0/19/0 to VLAN 1000.

```
huawei(config)#vlan 1000 smart
huawei(config)#port vlan 1000 0/19 0
```

6. Create service flows.

   Set the service VLAN to 1000, GEM port ID to 13, and user VLAN to 1000, and use traffic profile 8.

```
huawei(config)#service-port 1 vlan 1000 gpon 0/1/0 ont 1 gemport 13 multi-service
 user-vlan 1000 rx-cttr 8 tx-cttr 8
```

7. Create an MVLAN and configure the IGMP version.

   Set the IGMP version for the MVLAN to IGMPv2.

```
huawei(config)#multicast-vlan 1000
huawei(config-mvlan1000)#igmp version v2
  This operation will delete all IPv4 programs with source IP addresses in the
current multicast VLAN
  Are you sure to change current IGMP version? (y/n)[n]:y
  Command is being executed. Please wait...
  Command has been executed successfully
```

8. Configure a program library.

   Set the mode for obtaining multicast programs to dynamic.

   NOTE

   You can set the mode for obtaining multicast programs to dynamic only when the IGMP mode is off.

```
huawei(config-mvlan1000)#igmp mode off
  Are you sure to close IGMP? (y/n)[n]:y
  Command is being executed. Please wait...
  Command has been executed successfully

huawei(config-mvlan1000)#igmp match mode disable
  Command has been executed successfully
```


Copyright © Huawei Technologies Co., Ltd.

(Optional) Set the address range for the dynamic programs. If you need to limit the address range of dynamic programs, perform this operation. For example, set the address range of dynamic programs to 224.1.1.1-224.1.1.100.

```
huawei(config-mvlan1000)#igmp match group ip 224.1.1.1 to-ip 224.1.1.100
```

9. Set the IGMP mode.

   Select the IGMP proxy mode.

```
huawei(config-mvlan1000)#igmp mode proxy
  Are you sure to change IGMP mode? (y/n)[n]:y
  Command is being executed. Please wait...
  Command has been executed successfully
```

10. Configure the IGMP uplink port.

    Set the IGMP uplink port ID to 0/19/0 and working mode to **default**. Protocol packets are transmitted to all the IGMP uplink ports in the multicast VLAN.

```
huawei(config-mvlan1000)#igmp uplink-port 0/19/0
huawei(config-mvlan1000)#btv
huawei(config-btv)#igmp uplink-port-mode default
Are you sure to change the uplink port mode?(y/n)[n]:y
```

11. (Optional) Set multicast global parameters.

    In this example, the default settings are used for all the multicast global parameters.

12. Configure multicast users.

    Add service ports 1 and 2 as multicast users.

```
huawei(config-btv)#igmp user add service-port 1
huawei(config-btv)#multicast-vlan 1000
huawei(config-mvlan1000)#igmp multicast-vlan member service-port 1
huawei(config-mvlan1000)#quit
```

13. Save the data.

```
huawei(config)#save
```

- The ONU does not need to be configured.
- Configure the HGW.

  1. Log in to the web configuration window.

     a. Enter http://192.168.1.1/cu.html (default IP address) to the address bar of the Internet Explorer (IE) and press Enter.

     b. In the login dialog box, enter the user name and password of the administrator (the Internet service provider (ISP) provides the default user name and default password). Then, click **OK**.

  2. Set parameters for the BTV service.

     This example assumes LAN3 as a BTV port.

     a. Choose **Network** > **Bandwidth Configuration** from the navigation tree.

     b. In the right pane, create LAN connection 3 for the BTV service. Set the parameters as follows:

Parameter	Value
Bearing service	**OTHER**: The connection is used for the BTV service.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Value
VLAN enabling	**Enable** VLAN tags are added to upstream packets. **NOTE** When BTV service flows are created on the OLT, the value is **Disable** if **uservlan** is untagged and the value is **Enable** if **uservlan** is tagged.
VLANID [1-4094]	VLAN ID corresponding to the user VLAN value for BTV service flows created on the OLT. In this example, set this parameter to 43.
Binding item	LAN3
Mode	Bridge
DHCP transparent transmission	Enable

c. Click **OK** to save the settings.

3. Restart the HGW.

   Choose **Management** > **Device Management** and click **Restarting the Device**.

----End

10.6.1.11 Configuring the VoD Service

The OLT is connected to the remote bridging ONU through a GPON port to provide users with the VoD service.

Prerequisites

- The OLT is connected to the BRAS and the program source.
- The VLAN of the LAN switch port connected to the OLT is the same as the upstream VLAN of the OLT.
- The ONU has been added to the OLT. For details, see **10.6.1.3 Adding an ONU to an OLT**.
- A VDSL2 port has been activated. For details, see **10.6.1.4 Configuring a VDSL2 User Port**.

Data Plan

Item	Data
ONU line profile	Profile name: fttd T-CONT ID: 4 GEM port ID: 13

Copyright © Huawei Technologies Co., Ltd.

Item	Data
Traffic profile	ID: 8 802.1p priority: 4 CIR: off (unlimited) Priority-based scheduling policy: local-setting
VLAN Plan	Single VLAN tag: ● SVLAN ID: 1100 ● VLAN type: smart ● VLAN attribute: common ● UVLAN (upstream VLAN of the HGW): 43 ● CVLAN=UVLAN VLAN translation policy: ● ONU: transparently transmits the UVLAN of the HGW. ● OLT: implements VLAN translation: U<->S.

Procedure

Step 1 Configure the OLT.

1. Configure a traffic profile.

   Configure traffic profile 8. Set the CIR to off (unlimited), priority to 4, and priority-based scheduling policy to local-setting (that is, queues are scheduled based on the priority specified in the profile).

   NOTE

   Run the **display traffic table ip** command to query the existing traffic profiles in the system. If the existing traffic profiles in the system do not meet the requirements, run the **traffic table ip** command to add a traffic profile.

   ```
   huawei(config)#traffic table ip index 8 cir off priority 4 priority-policy
   local-setting
   ```

2. Configure the mapping relationship between a GEM port and a VDSL2 port on the ONU.

   The service flow of user VLAN 43 is mapped to GEM port 13 in the ONU line profile.

   ```
   huawei(config)#ont-lineprofile gpon profile-name fttd
   huawei(config-gpon-lineprofile-1)#gem mapping 13 4 vlan 43
   huawei(config-gpon-lineprofile-1)#commit
   huawei(config-gpon-lineprofile-1)#quit
   ```

3. Configure the VLAN of the Ethernet port on the ONU.

   If the ONU is connected to the HGW through VDSL2 port 1, add VDSL2 port 1 to VLAN 43.

   ```
   huawei(config)#ont-srvprofile gpon profile-name fttd
   huawei(config-gpon-srvprofile-1)#port vlan vdsl 1 43
   huawei(config-gpon-srvprofile-1)#commit
   huawei(config-gpon-srvprofile-1)#quit
   ```


Copyright © Huawei Technologies Co., Ltd.

4. Create a service VLAN and add an upstream port to it.

   Add upstream port 0/19/0 to VLAN 1100.

   ```
   huawei(config)#vlan 1100 smart
   huawei(config)#port vlan 1100 0/19 0
   ```

5. Create service flows.

   Set the service VLAN to 1100, GEM port ID to 13, and user VLAN to 43, and use traffic profile 8.

   ```
   huawei(config)#service-port 3 vlan 1100 gpon 0/1/0 ont 1 gemport 13
   multi-service user-vlan 43 rx-cttr 8 tx-cttr 8
   ```

6. Save the data.

   ```
   huawei(config)#save
   ```

Step 2 The ONU does not need to be configured.

Step 3 Configure the HGW.

1. Log in to the web configuration window.
   a. Enter http://192.168.1.1/cu.html (default IP address) to the address bar of the IE browser and press **Enter**.
   b. In the login dialog box, enter the user name and password of the administrator (the Internet service provider (ISP) provides the default user name and default password). Then, click **OK**.
2. Set parameters for the VoD service.

   This example assumes LAN4 as an VoD port.
   a. Choose **Network** > **Bandwidth Configuration** from the navigation tree.
   b. In the right pane, create LAN connection 4 for the VoD service. Set the parameters as follows:

Parameter	Value
Bearing service	**OTHER**: The connection is used for the VoD service.
VLAN enabling	**Enable** VLAN tags are added to upstream packets. **NOTE** When VoD service flows are created on the OLT, the value is **Disable** if **uservlan** is untagged and the value is **Enable** if **uservlan** is tagged.
VLANID [1-4094]	VLAN ID corresponding to the user VLAN value for VoD service flows created on the OLT. In this example, set this parameter to 43.
Binding item	LAN4
Mode	Bridge
DHCP transparent transmission	Enable

   c. Click **OK** to save the settings.

Copyright © Huawei Technologies Co., Ltd.

3. Restart the HGW.
   Choose **Management** > **Device Management** and click **Restarting the Device**.

----End

10.6.1.12 Verifying Services

In the FTTD scenario, ONUs are installed in users' houses which are far away from the central equipment room. ONUs provide remote service verification methods including PPPoE dialup emulation, call emulation, and multicast emulation to facilitate configuration and commissioning engineers to verify services remotely after service configuration.

Prerequisites

ONUs and upper-layer devices have been connected properly. The BRAS and MGC/IMS have been configured.

Background

Remote Service Verification Method	Function	Description
PPPoE dialup emulation	An ONU simulates a PPPoE user terminal software to perform dialup and interact with the BRAS to verify the connectivity between the ONU and BRAS.	● PPPoE dialup emulation requires a service flow which does not belong to a QinQ VLAN. ● A user name, password, and authentication mode must be configured on the BRAS for the PPPoE dialup emulation. ● An ONU supports a maximum of a PPPoE dialup emulation.
Call Emulation	An ONU simulates a voice user to make a call to check whether the voice service data is correctly configured. You can also use the call emulation function to locate a fault when the voice service is faulty.	● An ONU can simulate a caller or callee to communicate with a phone in a call. In this case, only a functional phone is required in the central office where the acceptance personnel is. ● An ONU supports a maximum of a call emulation.
Multicast emulation	This function enables you to simulate a multicast user going online and lead the program stream to an ONU. You can check whether the multicast service is normal by checking the real-time traffic of the multicast program.	Multicast services configured in the dynamic controllable multicast mode do not support this function.

Copyright © Huawei Technologies Co., Ltd.

Data plan

Item	Data	Remarks
PPPoE dialup emulation parameters	PPPoE user name: test@huawei Password: test	The user name, password, and authentication mode for the emulation test must be configured on the BRAS. The entered user name, password, and authentication mode must be consistent with those configured on the BRAS.
Call emulation parameters	ONU POTS ID: 1	The default values are used. You can run the **display pots emulational configuration** command to check the parameter values.
Multicast emulation parameters	Multicast service flow ID: 1 MVLAN: 1000 IP address of the multicast program: 224.1.1.10	-

Procedure

- Verify the Internet access service using PPPoE dialup emulation.
  1. In the xPON board mode, run the **pppoe simulate start** command to start a PPPoE dialup emulation test. The following test uses GPON as an example:

```
huawei(config)#interface gpon 0/1
huawei(config-if-gpon-0/1)#pppoe simulate start
{ portid<U><0,7> }:0
{ ontid<U><0,127> }:1
{ eth<K>|untagged<K>|vdsl|vlanid<U><0,4095> }:vdsl
{ ont-portid<U><1,8> }:1
{ untagged<K>|vlanid<U><0,4095> }:100
{ priority<U><0,7>|user-name<K> }:user-name
{ username<S><Length 1-64> }:test@huawei
{ user-password<K> }:user-password
{ password<S><Length 1-64> }:test
{ authentication-mode<K> }:authentication-mode
{ protocol<E><chap,pap> }:chap

  Command:
          pppoe simulate start 0 1 vdsl 1 100 user-name test@huawei user-
password
 test authentication-mode chap

huawei(config-if-gpon-0/1)#
  ---------------------------------
  ONT PPPoE Test Result
  ---------------------------------
  F/S/P                : 0/1/0
  ONT-ID               : 1
  ONT VDSL Port ID     : 1
  ONT Vlan ID          : 100
  Vlan Priority        : -
  Emluator result      : Success
   ---------------------------------
```


Copyright © Huawei Technologies Co., Ltd.

- Troubleshooting methods for the Internet access service
  1. Check whether configurations are complete on the OLT.
     - Run the **display ont info** command to query the ONU status to check whether the ONU is registered successfully.
     - Run the **display service-port** command to check whether the Internet access service flow is configured and whether the inner VLAN ID of the service flow is consistent with that in the data plan.
     - If a native VLAN is configured for the VDSL2 port on the ONU, run the **display ont port attribute** command in the xPON board mode to check whether the native VLAN is correct.
  2. Check the upstream and downstream ports by checking the MAC address learning status.
     a. Run the **display mac-address vlan** command to check the MAC address learning status of the Internet service VLAN.
        - If the upstream port does not learn a MAC address, check the network connections between the upstream port and upper-layer devices and check the configurations of upper-layer devices.
        - If the downstream port does not learn a MAC address, check whether the ONU is activated, whether the PC is connected to the right port on the ONU, and whether the PC is working properly.
     b. Run the **display ont-learned-mac** command to check whether the ONU connecting to the PON port learned any MAC addresses.

        If not, check whether the ONU properly connects to the PC or home gateway (HGW).
- Verify the voice service using call emulation.
  1. Run the **ont emulational call** command to configure a call emulation test.

```
huawei(config)#test
huawei(config-test)#ont emulational call caller-port 0/1/0 1 1 telno
28777192
{ <cr>|caller-stop-time<K> }:

  Command:
          ont emulational call caller-port 0/1/0 1 1 telno 28777192
```

  2. The ONU outputs the call emulation result after the test is complete.

```
huawei(config-test)#
  ------------------------------------------------------------------
  F/S/P                : 0/1/0
  ONT-ID               : 0
  ONT-POTS ID          : 1
  Test type            : caller emulational call test
  Detected number      : 28777192
  Reported number      : 28777192
  Current status       : test end
  Test Result          : success
  ------------------------------------------------------------------
```

- Troubleshooting methods for the voice service.
  1. Check whether configurations are complete on the OLT.
     - Run the **display ont info** command to query the ONU status to check whether the ONU is registered successfully.

Copyright © Huawei Technologies Co., Ltd.

- Run the **display service-port** command to check whether the voice service flow is configured and whether the inner VLAN ID of the service flow is consistent with that in the data plan.

2. Check the upstream and downstream ports by checking the MAC address learning status.

   Run the **display mac-address vlan** command to check the MAC address learning status of the voice service VLAN.

   - If the upstream port does not learn a MAC address, check the network connections between the upstream port and upper-layer devices and check the configurations of upper-layer devices.
   - If the downstream port does not learn a MAC address, check whether the ONU is activated and whether physical links are normal.
   - If both the upstream and downstream ports can learn the MAC address, record the MAC address of the ONU and log in to the service router (SR) to check whether an IP address is allocated to the MAC address.

3. Check the registration status of the voice service.

   - You can run the **display ont port state** command on the OLT to query the call connection status on the POTS port. If **Call State** is **RegisterFail** or **Connecting** for a long time, check whether the voice configuration on the MGC/SIP server is consistent with that on the ONU.
   - If the ONU uses the H.248 protocol, you can run the **display ont mg status** command on the OLT to query the registration status of the MG interface that connects to the ONU. If **MG Status** is **UnRegistered** or **Registering** for a long time, check whether the voice configuration on the MGC/SIP server is consistent with that on the ONU.
   - You can query the registration status of the voice service on the ONU web page. If the query result shows that the registration fails or the voice service is in the registering state for a long time, check whether the voice configuration on the MGC/SIP server is consistent with that on the ONU.

- Verify the multicast service using multicast emulation.

  1. Run the **igmp static-join** command to simulate a multicast user to order a multicast program.

     ```
     huawei(config)#btv
     huawei(config-btv)#igmp static-join service-port 1 ip 224.1.1.10 vlan 1000
     ```

     NOTE

     If the multicast program is obtained dynamically, **igmp static-join** can be executed successfully only when the range for obtaining the dynamic program is set.

  2. Run the **display igmp user** command to query the status of the multicast user.

     ```
     huawei(config-btv)#display igmp user service-port 1
       User                       : 0/1/0/1
       State                      : online
       Authentication             : no-auth
       Quick leave                : MAC-based
       IGMP flow ID               : 1
       Video flow ID              : 1
       Log switch                 : enable
       Bind profiles              : -
       IGMP version               : IGMP v3
       Current version            : IGMP v3
       Current IGMP IPv6 version  : IGMP IPv6 v2
     ```


Copyright © Huawei Technologies Co., Ltd.

```
  Available programs         : 8
  Global leave               : disable
  User max bandwidth         : no-limit
  Used bandwidth(kbps)       : 0
  Used bandwidth
  to max bandwidth(%)        : -
  Total video bandwidth      : -
  Mcast video bandwidth      : -
  Active program list

-------------------------------------------------------------------------
--
  Program name     VLAN  IP/MAC           State           Start time

-------------------------------------------------------------------------
--
  PROGRAM-5        1000  224.1.1.10       watching        2011-10-29
                                                         16:33:41+08:00

-------------------------------------------------------------------------
--
  Total: 1
```

3. Run the **display multicast flow-statistic** command to query the real-time traffic of the multicast program.

```
huawei(config-btv)#display multicast flow-statistic vlan 1000 ip
224.1.1.10
{ <cr>|sourceip<K> }:

  Command:
          display multicast flow-statistic vlan 1000 ip 224.1.1.10
  Command is being executed. Please wait...
  Multicast flow statistic result: 8736(kbps)
```

----End

10.6.2 Bridging ONU Network Scenario (MA5651/MA5651S)

This topic describes how to configure Internet access service, voice service, BTV service and VoD service when bridging ONUs are used to build an FTTD network.

10.6.2.1 Service Requirements and Application Scenario

Service Requirements

Optical fibers are connected to user homes and triple play services are required. The following provides detailed service requirements:

- Internet access of multiple PCs in a home is supported.
- Access of multiple telephones in a home is supported.
- IPTV programs can be previewed and watched using STBs.
- Service extension is supported and different services do not affect each other.
- Service faults are easy to locate and services are easy to maintain.

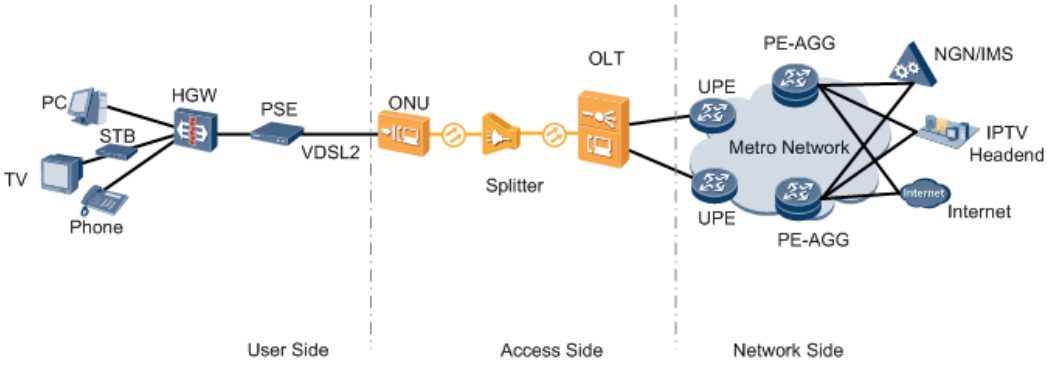
Application Scenario

As shown in **Figure 10-9**, the HGW integrating an IAD provides Internet, voice over Internet Protocol (VoIP), and Internet Protocol television (IPTV) services to users.

Copyright © Huawei Technologies Co., Ltd.

Services are mainly implemented on the HGW, and the bridging ONU works with the OLT to provide Layer 2 channels.

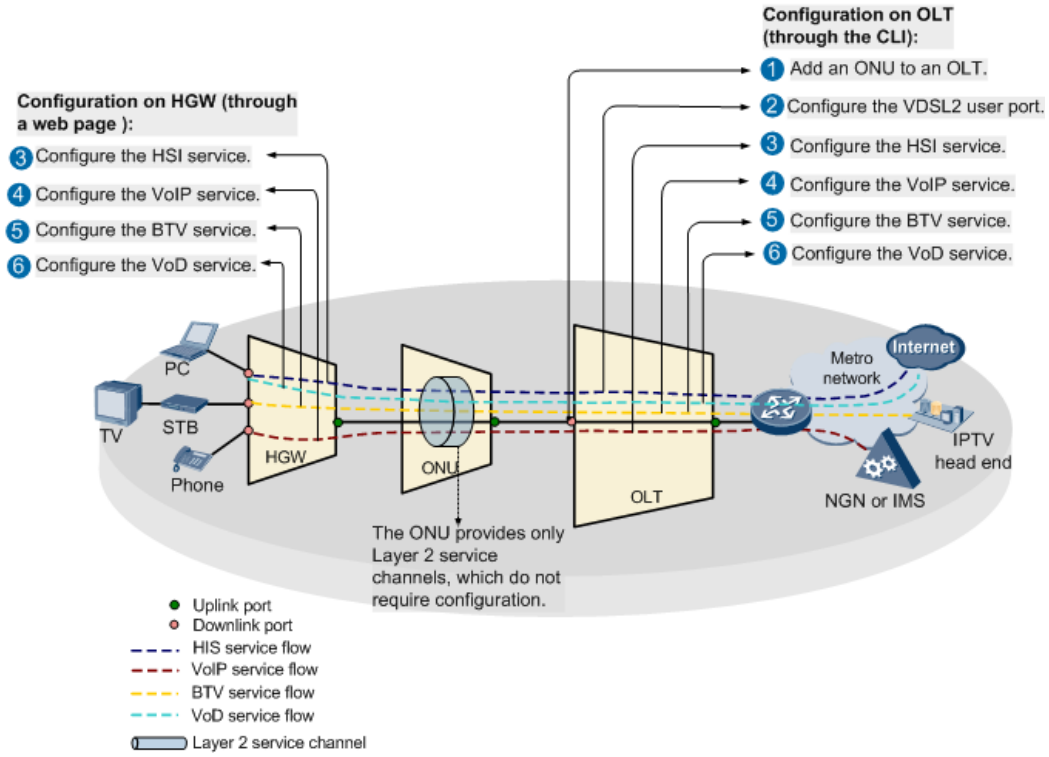
Figure 10-9 Bridging ONU + HGW



10.6.2.2 Configuration Process

Figure 10-10 shows the configuration roadmap in fiber to the door (FTTD) networking using a bridging optical network unit (ONU)+home gateway (HGW).

Figure 10-10 Configuration roadmap in FTTD networking using a bridging ONU+HGW



The following table describes the configuration steps.

Copyright © Huawei Technologies Co., Ltd.

Item	Step		Description
Optical line terminal (OLT)	**10.6.2.3 Adding an ONU to an OLT**		Services can be configured for an optical network unit (ONU) only after the ONU is added to an optical line terminal (OLT).
OLT	**10.6.1.4 Configuring a VDSL2 User Port**		Services can be transmitted only after a VDSL2 port on an optical network unit (ONU) is activated.
OLT HGW	**10.6.2.5 Configuring the Internet Access Service**		● An ONU provides only Layer 2 service channels, which do not require configuration. An HGW is equipped with an integrated access device (IAD) provides the Internet access, VoIP, and IPTV services for users. ● IPTV services include the BTV and VoD services that are different in configuration procedures and need to be configured separately.
	10.6.2.6 Configuring the Voice Service		
	Configure the IPTV service.	**10.6.2.7 Configuring the BTV Service**	
		10.6.2.8 Configuring the VoD Service	
OLT	**10.6.2.9 Verifying Services**		The OLT provides remote verification methods including ONT PPPoE/DHCP dialup emulation and multicast emulation for configuration and commissioning engineers to verify services remotely after service configuration, avoiding a second on-site operation.

10.6.2.3 Adding an ONU to an OLT

Services can be configured for an optical network unit (ONU) only after the ONU is added to an optical line terminal (OLT).

Data Plan

Table 10-5 Data plan

Item	Data
DBA profile	Profile name: fttd_dba Profile type: type3 Assured bandwidth: 8 Mbit/s Maximum bandwidth: 20 Mbit/s

Copyright © Huawei Technologies Co., Ltd.

Item	Data
ONU line profile	Profile name: fttd T-CONT ID: 4 GEM port ID for the management service: 11 GEM port ID for the voice service: 12 GEM port ID for the video service: 13 GEM port ID for the Internet access service: 14
ONU service profile	Profile name: fttd ONU port capability set: one VSDL2 port
Network topology data	PON port: 0/1/0 ONU IDs: 1

Procedure

Step 1 Configure GPON ONU profiles.

GPON ONU profiles include the DBA profile, line profile, service profile, and alarm profile.

- DBA profile: A DBA profile describes GPON traffic parameters. A T-CONT is bound to a DBA profile for dynamic bandwidth allocation, improving upstream bandwidth utilization.
- Line profile: A line profile describes the binding between the T-CONT and the DBA profile, the QoS mode of the traffic stream, and the mapping between the GEM port and the ONU-side service.
- Service profile: A service profile provides the service configuration channel for the ONU that is managed by using optical network terminal management and control interface (OMCI).
- Alarm profile: An alarm profile contains a series of alarm thresholds to measure and monitor the performance of activated ONU lines. When a statistical value reaches the threshold, the host is notified and an alarm is reported to the log host and the NMS.

1. Configure a DBA profile.

   Run the **display dba-profile** command to query existing DBA profiles in the system. If the existing DBA profiles in the system do not meet the requirements, run the **dba-profile add** command to add a DBA profile.

   Create the same DBA profile for different types of services. Set the profile name to **fttd_dba**, profile type to **type3**, assured bandwidth to 8 Mbit/s, and maximum bandwidth to 20 Mbit/s.

   ```
   huawei(config)#dba-profile add profile-name fttd_dba type3 assure 8192 max
   20480
   ```

   NOTE

   The DBA implementation is based on an ONU. Therefore, select a DBA profile of the proper bandwidth type and configure proper bandwidth according to the service types and total user count of the ONU. Note that the sum of the fixed bandwidth and the assured bandwidth must not be greater than the total bandwidth of the PON port.

Copyright © Huawei Technologies Co., Ltd.

2. Configure an ONU line profile.

   Create a GPON ONU line profile, named **fttd**, and bind it to the DBA profile **fttd_dba**.

   ```
   huawei(config)#ont-lineprofile gpon profile-name fttd
   huawei(config-gpon-lineprofile-1)#tcont 4 dba-profile-name fttd_dba
   ```

   Create different GEM ports according to different service types, in which

   - GEM port 11 is used to carry management services.
   - GEM port 12 is used to carry voice services.
   - GEM port 13 is used to carry video services.
   - GEM port 14 is used to carry Internet access services.

   ```
   huawei(config-gpon-lineprofile-1)#gem add 11 eth tcont 4
   huawei(config-gpon-lineprofile-1)#gem add 12 eth tcont 4
   huawei(config-gpon-lineprofile-1)#gem add 13 eth tcont 4
   huawei(config-gpon-lineprofile-1)#gem add 14 eth tcont 4
   ```

   NOTE

   1. To change the default QoS mode, run the **qos-mode** command to set the QoS mode to **gem-car** or **flow-car**, and run the **gem add** command to set the index of the traffic profile bound to the GEM port.
   2. When the QoS mode is priority-queue (PQ), the default queue priority is 0; when the QoS mode is flow-car or gem-car, traffic profile 6 is bound to the GEM port by default (no rate limitation).

   After the configurations are complete, run the **commit** command to apply the parameter settings.

   ```
   huawei(config-gpon-lineprofile-1)#commit
   huawei(config-gpon-lineprofile-1)#quit
   ```

3. Configure an ONU service profile.

   Create a GPON ONU service profile, named **fttd**. Configure the capability set of the VDSL2 port and POTS port to **1** and **2**. Then the system automatically adapts to the ONU according to the actual capability of the online ONU.

   ```
   huawei(config)#ont-srvprofile gpon profile-name fttd
   huawei(config-gpon-srvprofile-1)#ont-port vdsl 1
   ```

   After the configurations are complete, run the **commit** command to apply the parameter settings.

   ```
   huawei(config-gpon-srvprofile-1)#commit
   huawei(config-gpon-srvprofile-1)#quit
   ```

4. (Optional) Add an alarm profile.

   - The default GPON alarm profile 1 is used. The alarm thresholds of the default alarm profile are 0, which indicates that no alarm is generated.
   - In this example, the default alarm profile is used, and therefore the configuration of the alarm profile is not required.
   - Run the **gpon alarm-profile add** command to configure a GPON alarm profile, which is used for monitoring the performance of an activated ONU line.

Step 2 Add an ONU.

Connect one ONU to GPON port 0/1/0. Set the ONU ID to **1**, password to **0100000001**, discovery mode for password authentication to **once-on**, and management mode to **OMCI**. Bind the ONU to ONU line profile **fttd** and ONU service profile **fttd**.

There are two methods of adding an ONU: add an ONU offline and confirm an automatically discovered ONU.

Copyright © Huawei Technologies Co., Ltd.

- Add ONUs offline.

  If the password of an ONU is known, run the **ont add** command to add an ONU offline.

```
huawei(config)#interface gpon 0/1
huawei(config-if-gpon-0/1)#ont add 0 1 password-auth 0100000001 once-on no-aging
omci ont-lineprofile-name
 fttd ont-srvprofile-name fttd
```

- Confirm automatically discovered ONUs

  If the password or SN of an ONU is unknown, run the **port *portid* ont-auto-find enable** command in GPON mode to enable the ONU auto-discovery function of the GPON port. Then, run the **ont confirm** command to confirm the ONU.

```
huawei(config)#interface gpon 0/1
huawei(config-if-gpon-0/1)#port 0 ont-auto-find enable
huawei(config-if-gpon-0/1)#display ont autofind 0
  //After this command is executed, the information about all ONUs connected to
the GPON port through optical splitters is displayed.

huawei(config-if-gpon-0/1)#ont confirm 0 ontid 1 password-auth 0100000001 once-
on no-aging omci ont-lineprofile-name
 fttd ont-srvprofile-name fttd
```

  NOTE

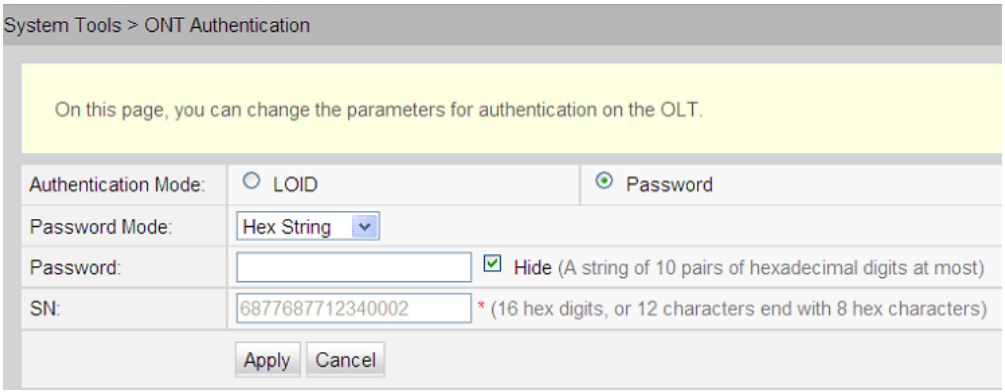
  If multiple ONUs of the same type bound to the same line profile or service profile are connected to the same port, you can bulk add ONUs by bulk confirming automatically discovered ONUs to make configuration easier and more efficient. To do so, the preceding command can be modified as follows:

```
huawei(config-if-gpon-0/1)#ont confirm 0 all password-auth once-on no-aging omci
ont-lineprofile-name fttd
ont-srvprofile-name fttd
```

  NOTE

  The password entered when you add an ONU to the OLT must be the same as that configured on the web page. To configure the password of the ONU on the web page, see **Figure 10-11**.

Figure 10-11 Modifying ONU password on the web page



- (Optional) Bind the alarm profile to the ONU.

  The default profile 1 is used in this example.

```
huawei(config-if-gpon-0/1)#ont alarm-profile 0 1 profile-id 1
```

Step 3 Check ONU status.

After an ONU is added, run the **display ont info** command to query the current status of the ONU. Ensure that **Config flag** of the ONU is **active**, **Run State** is **online**, **Config state** is **normal**, and **Match state** is **match**.

```
huawei(config-if-gpon-0/1)#display ont info 0 1
  ------------------------------------------------------------------------
```


Copyright © Huawei Technologies Co., Ltd.

```
  F/S/P                : 0/1/0
  ONT-ID               : 1
  Control flag         : active    //Indicates that the ONU is
activated.
  Run state            : online    //Indicates that the ONU goes online
successfully.
  Config state         : normal    //Indicates that the configuration state of the
ONU is normal.
  Match state          : match     //Indicates that the capability profile bound to
the ONU is consistent with the actual capability of the ONU.
...//The rest of the response information is omitted.
```

When **Config state** is **failed**, **Run state** is **offline**, or **Match state** is **mismatch**:

- If **Control flag** is **deactive**, run the **ont active** command in GPON mode to activate the ONU.
- If **Run state** is **offline**, a physical line may be broken or the optical module may be damaged. Check the line and the optical module.
- If **Config state** is **failed**, the configured ONU capability exceeds the actual ONU capability. In this case, run the **display ont failed-configuration** command in the diagnose mode to check the failed configuration item and the failure cause. Then, rectify the fault accordingly.

----End

10.6.2.4 Configuring a VDSL2 User Port

Services can be transmitted only after a VDSL2 port is activated on an optical network unit (ONU). This section describes how to activate a VDSL2 port and bind a VSDL2 line profile to the port.

Prerequisites

- An ONU has been added to the optical line terminal (OLT). For details, see **10.6.1.3 Adding an ONU to an OLT**.
- Run the **display xdsl mode** command to check whether the VDSL2 mode is the desired mode. The default mode is TR129. If the current mode is not the desired one, run the **switch vdsl mode to** command in diagnose mode to switch the mode to the desired mode.

  NOTE

  - A fiber to the door (FTTD) network supports only the TR129 and TR165 modes.
  - G.INP takes effect preferentially if both G.INP and SRA are enabled.

Typical VDSL2 Line Parameter Configurations

Key parameters to be configured do not vary with the VDSL2 mode but belong to different profiles. Hence, commands for configuring the key parameters vary with the VDSL2 mode.

Table 10-6 lists the typical configurations for key parameters of a VDSL2 line (26 AWG, 0.4 mm twisted pair). Information provided in this table is for reference only. Usually, take the default values for the other parameters.

Copyright © Huawei Technologies Co., Ltd.

Table 10-6 Typical configurations for key parameters of a VDSL2 line (0.4 mm twisted pair)

Parameter	Access Distance					Remarks
	< 100 m	< 300 m	300-500 m	500-800 m	800-1000 m	
Selected VDSL2 profile	30a	17a	12a	8b, 12a	8b	A 30a VDSL2 profile is recommended on an FTTD network.
PSD mask	B8-16 (998-M2x-B)	B8-11 (998ADE17-M2x-A)	B8-6 (998-M2x-B)	B8-6 (998-M2x-B)	B8-6 (998-M2x-B)	None
Enable US0 (U0)	No	Yes	Yes	Yes	Yes	Enable US0 if the distance is longer than 500 m.
Maximum transmit rate downstream	100 Mbit/s	50 Mbit/s	40 Mbit/s	25 Mbit/s	20 Mbit/s	● Limiting the upstream and downstream rates ensures a higher signal-to-noise ratio (SNR) margin for the line and therefore enhances its capability for withstanding noise and interference. ● The rates can be specified using these two parameters and also can be

Copyright © Huawei Technologies Co., Ltd.

Parameter	Access Distance					Remarks
	< 100 m	< 300 m	300-500 m	500-800 m	800-1000 m	
Maximum transmit rate upstream	15 Mbit/s	15 Mbit/s	10 Mbit/s	5 Mbit/s	2 Mbit/s	specified in the traffic profile. When they are specified in both ways, the actual activation rate is determined by the smaller one.
Minimum INP	2 symbols	2 symbols	2 symbols	2 symbols	2 symbols	None
Target SNR margin	8 dB	8 dB	8 dB	8 dB	8 dB	None

Copyright © Huawei Technologies Co., Ltd.

Parameter	Access Distance					Remarks
	< 100 m	< 300 m	300-500 m	500-800 m	800-1000 m	
Path mode	PTM	PTM	PTM	PTM	PTM	Only the PTM mode is supported on an FTTD network.

Configuration Process

Figure 10-12 shows the process for configuring a VDSL2 line profile in TR129 mode.

Figure 10-12 Flowchart for configuring a VDSL2 line profile in TR129 mode

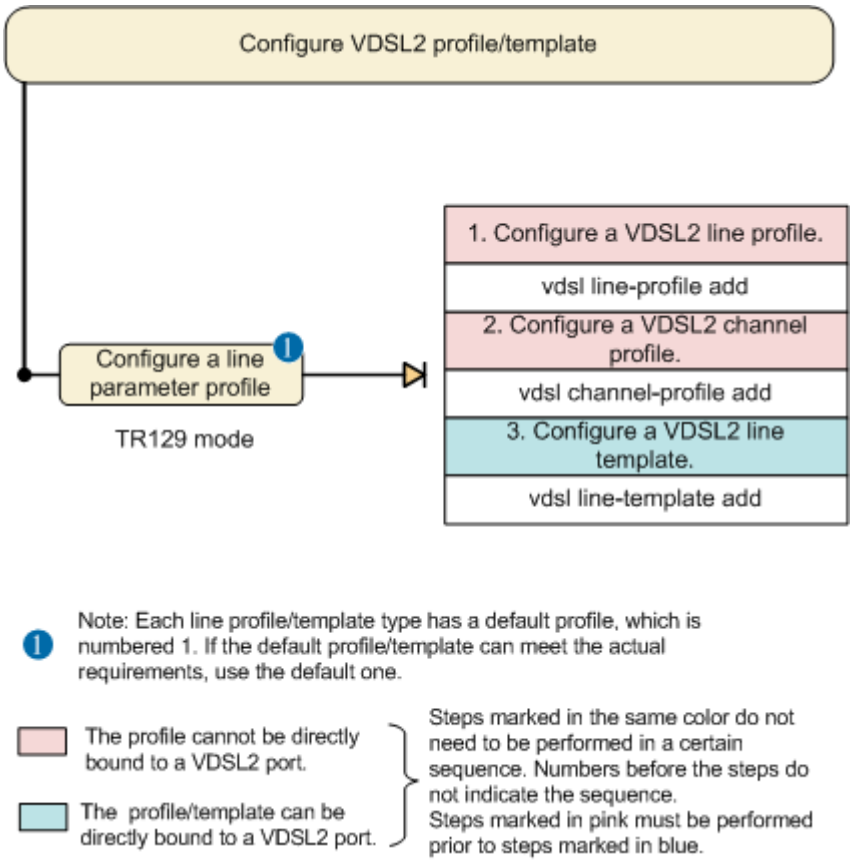
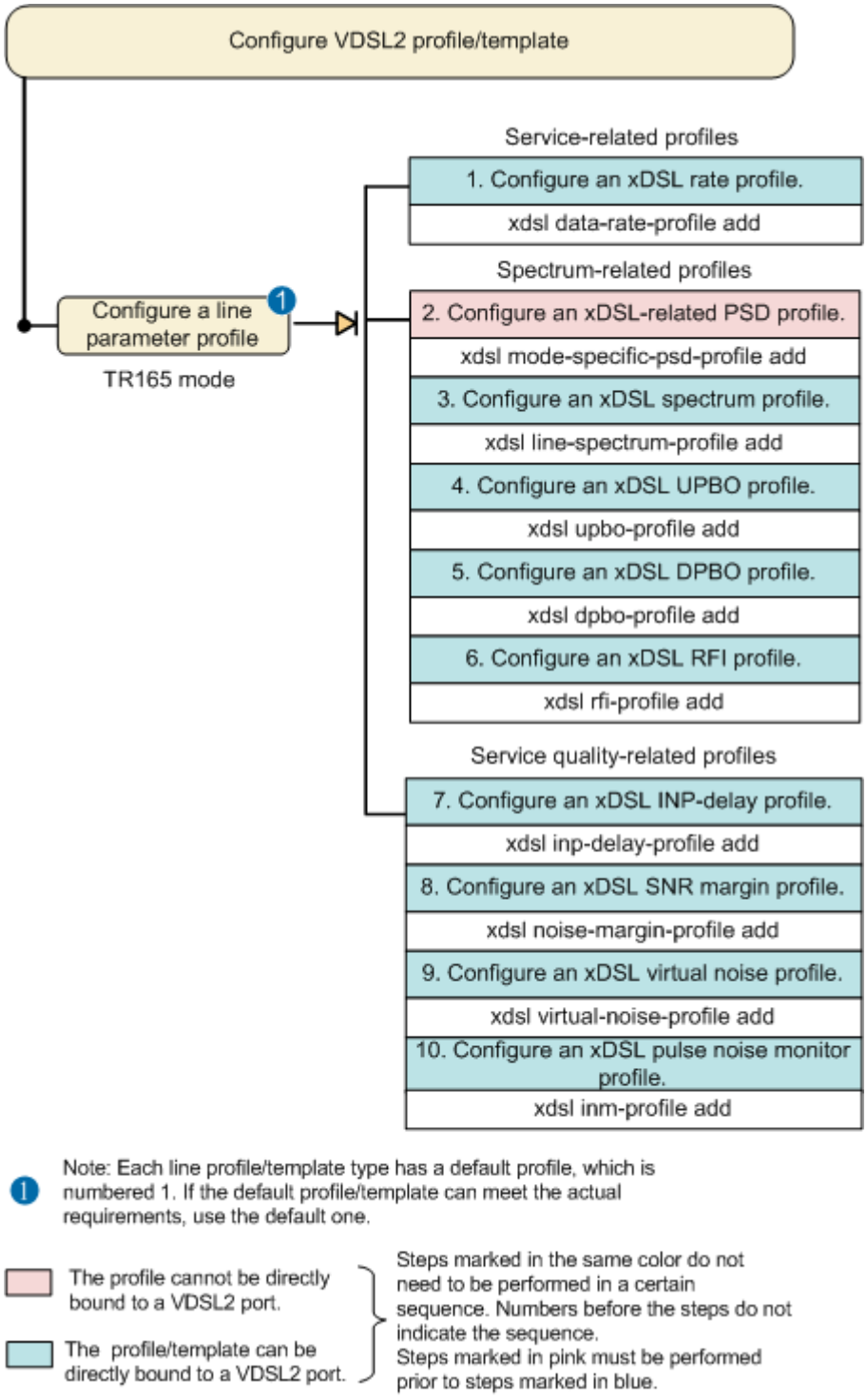


Figure 10-13 shows the process for configuring a VDSL2 line profile in TR165 mode.

Copyright © Huawei Technologies Co., Ltd.

Figure 10-13 Flowchart for configuring a VDSL2 line profile in TR165 mode



Procedure

Step 1 (Optional) Run the command in **Figure 10-12** or **Figure 10-13** to configure a VDSL2 line profile.

Copyright © Huawei Technologies Co., Ltd.

Perform this step if the default line profile (ID: 1) cannot meet site requirements. In this section, the default line profile is used.

Step 2 Activate a VDSL2 port and bind the VDSL2 line profile to the port.

Perform this step after the ONU becomes functional. The PON port data is shown in the following table.

Networking data	PON port: 0/1/0
	ONU ID: 1

In TR129 mode:

```
huawei(config-if-gpon-0/1)#ont port activate 0 1 vdsl-port 1 template-index 1
```

In TR165 mode:

```
huawei(config-if-gpon-0/1)#ont port activate 0 1 vdsl-port 1
```

----End

10.6.2.5 Configuring the Internet Access Service

An optical line terminal (OLT) is connected to a remote optical network unit (ONU) through a GPON port to provide users with high-speed Internet access services.

Prerequisites

- The OLT is connected to the BRAS.
- Related configurations are performed on the BRAS according to the authentication and accounting requirements for dialup users. For details about the configuration, see the configuration guide.
- The ONU has been added to the OLT. For details, see **10.6.1.3 Adding an ONU to an OLT**.
- A VDSL2 port has been activated. For details, see **10.6.1.4 Configuring a VDSL2 User Port**.
- The VLAN of the LAN switch port connected to the OLT is consistent with the upstream VLAN of the OLT.
- Residential users generally access the Internet through PPPoE dialup. PPPoE dialup can be performed on PCs or HGWs.
- The configuration processes on HGWs of different models or in different appearances are similar. This section describes how to configure the Internet access service on an HG239 that is connected to an ONU upstream through a LAN.

Copyright © Huawei Technologies Co., Ltd.

Data Plan

Item	Data
ONU line profile	Profile name: fttd T-CONT ID: 4 GEM port ID for Internet access service: 14
Network topology data	Uplink port: 0/19/0 PON port: 0/1/0 ONU IDs: 1 ID of the port on the HGW that is connected to the PC: 1
VLAN Plan	Double-tagged VLAN: ● S-VLAN ID: 100 ● S-VLAN type: smart ● S-VLAN attribute: stacking ● C-VLAN ID: 1001-1002 ● U-VLAN ID: 45 VLAN translation policy: ● ONU: transparently transmits the user VLAN tags carried in the upstream packets sent from the HGW. ● OLT: translates the user VLAN tags to S-VLAN+C-VLAN tags.

Procedure

- Configure the OLT.
  1. Configure a traffic profile.

     Configure traffic profile 8. Set the CIR to off (unlimited), priority to 4, and priority-based scheduling policy to local-setting (that is, queues are scheduled based on the priority specified in the profile).

     NOTE

     Run the **display traffic table ip** command to query the existing traffic profiles in the system. If the existing traffic profiles in the system do not meet the requirements, run the **traffic table ip** command to add a traffic profile.

     ```
     huawei(config)#traffic table ip index 8 name fttd_hsi cir off priority 4 priority-policy local-setting
     ```

  2. Configure the mapping between a GEM port and a VLAN.

     The service flow of user-side VLAN 45 is mapped to GEM port 14 in the ONU line profile.

     NOTE

     Here, the user-side VLAN is the VLAN carried by packets sent from HGW to ONU, namely, U-VLAN.

Copyright © Huawei Technologies Co., Ltd.

```
huawei(config)#ont-lineprofile gpon profile-name fttd
huawei(config-gpon-lineprofile-1)#gem mapping 14 0 vlan 45
huawei(config-gpon-lineprofile-1)#commit
huawei(config-gpon-lineprofile-1)#quit
```

3. Configure the VLAN of the Ethernet port on the ONU.

   Add Ethernet port 1 to VLAN 45 in the ONU service profile.

```
huawei(config)#ont-srvprofile gpon profile-name fttd
huawei(config-gpon-srvprofile-1)#port vlan eth 1 45
huawei(config-gpon-srvprofile-1)#commit
```

4. Create an Internet access service VLAN and add an uplink port to it.

   Add uplink port 0/19/0 to VLAN 100.

```
huawei(config)#vlan 100 smart
huawei(config)#vlan attrib 100 stacking
huawei(config)#port vlan 100 0/19 0
```

5. Create Internet access service flows.

   Set S-VLAN ID to 100 and GEM port ID to 14. Use traffic profile fttd_hsi.

```
huawei(config)#service-port vlan 100 gpon 0/1/0 ont 1 gemport 14 multi-
service
user-vlan 45 tag-transform translate-and-add inner-vlan 1001 inbound
traffic-table
 name fttd_hsi outbound traffic-table name fttd_hsi
```

6. Save the data.

```
huawei(config)#save
```

- Configure the HGW.

1. Log in to the web configuration window.

   a. Enter http://192.168.1.1/cu.html (default IP address) to the address bar of the IE browser and press **Enter**.

   b. In the login dialog box, enter the user name and password of the administrator (the Internet service provider (ISP) provides the default user name and default password). Then, click **OK**.

2. Set parameters for the Internet access service.

   Assume that ports LAN1 and LAN2 are Internet access ports for PCs.

   a. Choose **Network** > **Bandwidth Configuration** from the navigation tree.

   b. Create WAN connection 1 and set parameters based on the following table.

Parameter	Value
Bearing service	INTERNET
VLAN enabling	Enabled: Upstream packets contain VLAN tags. Disabled: Upstream packets do not contain VLAN tags. **NOTE** If **uservlan** is set to **untagged** when you configure a service flow for the Internet access service on the OLT, set this parameter to **Disabled**; otherwise, set it to **Enabled**.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Value
VLANID [1-4094]	If **VLAN enabling** is set to **Enabled**, this parameter takes the value of **uservlan** that is specified when you configure a service flow for the Internet access service on the OLT.
Binding item	LAN1 and LAN2: PCs connected to ports LAN1 and LAN2 can simultaneously access the Internet.
Mode	Bridge: PCs access the Internet through PPPoE dialup.

c. Click **OK**.

3. Restart the HGW.
   Choose **Management** > **Device Management** and click **Restarting the Device**.

----End

10.6.2.6 Configuring the Voice Service

The OLT is connected to the remote ONU through a GPON port to provide users with the IP-based high-quality and low-cost VoIP service.

Prerequisites

- The SIP interface data and POTS user data corresponding to the MG interface have been configured on the SIP server.
- The connection between the OLT and the SIP server is set up. The OLT can ping the IP address of the SIP server successfully.
- The ONU has been added to the OLT. For details, see **10.6.1.3 Adding an ONU to an OLT**.
- HGWs have different models and appearances but their configuration procedures are similar. This topic uses the HG255 that uses LAN for upstream transmission as examples.
- The IADs use SIP as the voice protocol.

Data Plan

Item	Data
ONU line profile	Profile name: fttd T-CONT ID: 4 GEM port ID: 12

Copyright © Huawei Technologies Co., Ltd.

Item	Data
VLAN plan	Single VLAN tag: ● VLAN ID: 300 ● VLAN type: smart ● VLAN attribute: common ● UVLAN ID: 45 VLAN translation policy: ● ONU: Upstream packets of the HGW carry the user VLAN and the ONU transparently transmits the packets. ● OLT: implements VLAN translation: U<->S.
Voice parameter	IP address of the SIP server: 200.200.200.200/24 Port ID of the SIP server: 5060 User phone number: 77730010

Procedure

- Configure the OLT.
  1. Configure a traffic profile.

     Run the **display traffic table ip** command to query the existing traffic profiles in the system. If the existing traffic profiles in the system do not meet the requirements, run the **traffic table ip** command to add a traffic profile.

     Set the profile name to **fttd_voip** and do not limit the upstream and downstream rates. Set the priority to **5** and packets are scheduled according to the priority carried.

     ```
     huawei(config)#traffic table ip name fttd_voip cir off priority 5 priority-policy
      local-setting
     ```

  2. Configure the mapping relationship between a GEM port and a VLAN.

     The service flow of user VLAN 45 is mapped to GEM port 12 in the ONU line profile.

     NOTE

     The user VLAN is the VLAN in the packets sent from the HGW to the ONU, that is, the UVLAN.

     ```
     huawei(config)#ont-lineprofile gpon profile-name fttd
     huawei(config-gpon-lineprofile-1)#gem mapping 12 2 vlan 45
     huawei(config-gpon-lineprofile-1)#commit
     huawei(config-gpon-lineprofile-1)#quit
     ```

  3. Configure the VLAN of the VDSL2 port on the ONU.

     If the ONU is connected to the HGW through VDSL2 port 1, add VDSL2 port 1 to VLAN 45 in the ONU service profile.

     ```
     huawei(config)#ont-srvprofile gpon profile-name fttd
     huawei(config-gpon-srvprofile-1)#port vlan vdsl 1 45
     huawei(config-gpon-srvprofile-1)#commit
     huawei(config-gpon-srvprofile-1)#quit
     ```


Copyright © Huawei Technologies Co., Ltd.

4. Create a service VLAN and add an upstream port to it.

   Add upstream port 0/19/0 to VLAN 300.

   ```
   huawei(config)#vlan 300 smart
   huawei(config)#port vlan 300 0/19 0
   ```

5. Create service flows.

   Set the service VLAN to 300, GEM port ID to 12, and user VLAN to 45, and use traffic profile **fttd_voip**.

   ```
   huawei(config)#service-port vlan 300 gpon 0/1/0 ont 1 gemport 12 multi-service
    user-vlan 45 inbound traffic-table name fttd_voip outbound traffic-table name
   fttd_voip
   ```

6. Enable the ARP proxy function.

   Voice media streams for different users of the same SVLAN fail to interchange because the service ports of the smart VLAN are isolated from each other. Therefore, the ARP proxy function needs to be enabled on the OLT.

   ```
   huawei(config)#arp proxy enable
   huawei(config)#interface vlanif 300
   huawei(config-if-vlanif300)#arp proxy enable
   huawei(config-if-vlanif300)#quit
   ```

7. Save the data.

   ```
   huawei(config)#save
   ```

- Configure the HGW.

  1. Log in to the Web configuration interface.

     a. Enter **http://192.168.1.1** (default IP address) in the address bar of the browser and press Enter.

     b. In the login window, enter the user name and password (the default value is provided by ISP) of the administrator and click **OK**.

  2. Configure parameters of the voice service.

     The configuration procedure is as follows:

     a. In the Web page, choose **Network** > **Bandwidth Configuration** from the navigation tree.

     b. Create WAN Connection 2 for the VoIP service and set the parameters as follows:

Parameter	Value
Bearing service	VoIP
Enabling status	Enable
VLAN mode	VLAN Transparent Transmission
VLAN ID	VLAN ID corresponding to the user VLAN value for voice service flows created on the OLT. In this example, set this parameter to 45.
802.1p	Enabled

Copyright © Huawei Technologies Co., Ltd.

Parameter	Value
Mode	Route: route mode
DHCP	Enabled
NAT	Enabled

c. Click **OK** to save the settings.

d. Choose **Appliciation** > **Broadband Phone Configuration** from the navigation tree. Configure the parameters as follows:

Parameter	Value
Address	Preferred IP address of the proxy server: 200.200.200.200
Port ID	Preferred signaling port ID of the proxy server: 5060
Enabling	Enabled
User number	When logging in to a VoIP account, you can set the user account to the user telephone number. In this example, set the user telephone number to 77730010.
User password	-

3. Restart the HGW.

   Choose **Management** > **Device Management** and click **Restarting the Device**.

----End

10.6.2.7 Configuring the BTV Service

The OLT is connected to the remote bridging ONU through a GPON port to provide users with the multicast service.

Prerequisites

- The OLT is connected to the BRAS and the multicast source.
- The VLAN of the LAN switch port connected to the OLT is the same as the upstream VLAN of the OLT.
- The ONU has been added to the OLT. For details, see **10.6.2.3 Adding an ONU to an OLT**.
- A VDSL2 port has been activated. For details, see **10.6.1.4 Configuring a VDSL2 User Port**.

Copyright © Huawei Technologies Co., Ltd.

Data Plan

Table 10-7 Data plan

Item	Data
ONU line profile	Profile name: fttd T-CONT ID: 4 GEM port ID: 13
Traffic profile	ID: 8 802.1p priority: 4 CIR: off (unlimited) Priority-based scheduling policy: local-setting
VLAN Plan	Single VLAN tag: ● SVLAN ID: 1000 ● HGW VLAN: 43 ● MVLAN ID: 1000 ● VLAN type: smart ● VLAN attribute: common VLAN translation policy: ● ONU: translates the user VLAN tags carried in the upstream packets sent from the HGW to MVLAN tags. ● OLT: duplicates multicast packets based on PON ports with MVLAN unchanged.
Multicast service data	Multicast protocol: IGMP proxy Multicast version: IGMPv2 Multicast program: dynamic obtaining mode

Procedure

- Configure the OLT.
  1. Configure a traffic profile.

     Configure traffic profile 8. Set the CIR to off (unlimited), priority to 4, and priority-based scheduling policy to local-setting (that is, queues are scheduled based on the priority specified in the profile).

     NOTE

     Run the **display traffic table ip** command to query the existing traffic profiles in the system. If the existing traffic profiles in the system do not meet the requirements, run the **traffic table ip** command to add a traffic profile.

     ```
     huawei(config)#traffic table ip index 8 cir off priority 4 priority-policy
     local-setting
     ```


Copyright © Huawei Technologies Co., Ltd.

2. Configure the mapping relationship between a GEM port and a VDSL2 port on the ONU.

   In the ONU line profile, the service flow of the VDSL2 port is mapped to GEM port 13.

```
huawei(config)#ont-lineprofile gpon profile-name fttd
huawei(config-gpon-lineprofile-1)#gem mapping 13 1 vlan 1000
huawei(config-gpon-lineprofile-1)#commit
huawei(config-gpon-lineprofile-1)#quit
```

3. Configure the VLAN of the VDSL2 port on the ONU.

   If the ONU is connected to the STB through VDSL2 port 2, add Ethernet port 2 to VLAN 1000.

```
huawei(config)#ont-srvprofile gpon profile-name fttd
huawei(config-gpon-srvprofile-1)#port vlan vdsl 1 translation 1000 user-
vlan 43
huawei(config-gpon-srvprofile-1)#multicast-forward tag translation 43
huawei(config-gpon-srvprofile-1)#commit
huawei(config-gpon-srvprofile-1)#quit
```

4. Configure the native VLAN of the ONU port.

   If the ONU is connected to the STB through VDSL2 port 1, the native VLAN ID is 1000.

```
huawei(config)#interface gpon 0/1
huawei(config-if-gpon-0/1)#ont port native-vlan 0 1 vdsl 1 vlan 1000
huawei(config-if-gpon-0/1)#quit
```

5. Create a service VLAN and add an uplink port to it.

   Add uplink port 0/19/0 to VLAN 1000.

```
huawei(config)#vlan 1000 smart
huawei(config)#port vlan 1000 0/19 0
```

6. Create service flows.

   Set the service VLAN to 1000, GEM port ID to 13, and user VLAN to 1000, and use traffic profile 8.

```
huawei(config)#service-port 1 vlan 1000 gpon 0/1/0 ont 1 gemport 13 multi-
service
 user-vlan 1000 rx-cttr 8 tx-cttr 8
```

7. Create an MVLAN and configure the IGMP version.

   Set the IGMP version for the MVLAN to IGMPv2.

```
huawei(config)#multicast-vlan 1000
huawei(config-mvlan1000)#igmp version v2
  This operation will delete all IPv4 programs with source IP addresses in
the
current multicast VLAN
  Are you sure to change current IGMP version? (y/n)[n]:y
  Command is being executed. Please wait...
  Command has been executed successfully
```

8. Configure a program library.

   Set the mode for obtaining multicast programs to dynamic.

   NOTE

   You can set the mode for obtaining multicast programs to dynamic only when the IGMP mode is off.

Copyright © Huawei Technologies Co., Ltd.

```
huawei(config-mvlan1000)#igmp mode off
  Are you sure to close IGMP? (y/n)[n]:y
  Command is being executed. Please wait...
  Command has been executed successfully

huawei(config-mvlan1000)#igmp match mode disable
  Command has been executed successfully
```

(Optional) Set the address range for the dynamic programs. If you need to limit the address range of dynamic programs, perform this operation. For example, set the address range of dynamic programs to 224.1.1.1-224.1.1.100.

```
huawei(config-mvlan1000)#igmp match group ip 224.1.1.1 to-ip 224.1.1.100
```

9. Set the IGMP mode.

   Select the IGMP proxy mode.

   ```
   huawei(config-mvlan1000)#igmp mode proxy
     Are you sure to change IGMP mode? (y/n)[n]:y
     Command is being executed. Please wait...
     Command has been executed successfully
   ```

10. Configure the IGMP uplink port.

    Set the IGMP uplink port ID to 0/19/0 and working mode to **default**. Protocol packets are transmitted to all the IGMP uplink ports in the multicast VLAN.

    ```
    huawei(config-mvlan1000)#igmp uplink-port 0/19/0
    huawei(config-mvlan1000)#btv
    huawei(config-btv)#igmp uplink-port-mode default
    Are you sure to change the uplink port mode?(y/n)[n]:y
    ```

11. (Optional) Set multicast global parameters.

    In this example, the default settings are used for all the multicast global parameters.

12. Configure multicast users.

    Add service ports 1 and 2 as multicast users.

    ```
    huawei(config-btv)#igmp user add service-port 1
    huawei(config-btv)#multicast-vlan 1000
    huawei(config-mvlan1000)#igmp multicast-vlan member service-port 1
    huawei(config-mvlan1000)#quit
    ```

13. Save the data.

    ```
    huawei(config)#save
    ```

- The ONU does not need to be configured.
- Configure the HGW.
  1. Log in to the web configuration window.
     a. Enter http://192.168.1.1/cu.html (default IP address) to the address bar of the Internet Explorer (IE) and press Enter.
     b. In the login dialog box, enter the user name and password of the administrator (the Internet service provider (ISP) provides the default user name and default password). Then, click **OK**.
  2. Set parameters for the BTV service.

     This example assumes LAN3 as a BTV port.

     a. Choose **Network** > **Bandwidth Configuration** from the navigation tree.
     b. In the right pane, create LAN connection 3 for the BTV service. Set the parameters as follows:

Copyright © Huawei Technologies Co., Ltd.

Parameter	Value
Bearing service	**OTHER**: The connection is used for the BTV service.
VLAN enabling	**Enable** VLAN tags are added to upstream packets. **NOTE** When BTV service flows are created on the OLT, the value is **Disable** if **uservlan** is untagged and the value is **Enable** if **uservlan** is tagged.
VLANID [1-4094]	VLAN ID corresponding to the user VLAN value for BTV service flows created on the OLT. In this example, set this parameter to 43.
Binding item	LAN3
Mode	Bridge
DHCP transparent transmission	Enable

c. Click **OK** to save the settings.

3. Restart the HGW.

   Choose **Management** > **Device Management** and click **Restarting the Device**.

----End

10.6.2.8 Configuring the VoD Service

The OLT is connected to the remote bridging ONU through a GPON port to provide users with the VoD service.

Prerequisites

- The OLT is connected to the BRAS and the program source.
- The VLAN of the LAN switch port connected to the OLT is the same as the upstream VLAN of the OLT.
- The ONU has been added to the OLT. For details, see **10.6.1.3 Adding an ONU to an OLT**.
- A VDSL2 port has been activated. For details, see **10.6.1.4 Configuring a VDSL2 User Port**.
- The configuration processes on HGWs of different models or in different appearances are similar. This topic describes how to configure the Internet access service on an HG239 that is connected to an ONT upstream through a LAN.

Copyright © Huawei Technologies Co., Ltd.

Data Plan

Item	Data
ONU line profile	Profile name: fttd T-CONT ID: 4 GEM port ID: 13
Traffic profile	ID: 8 802.1p priority: 4 CIR: off (unlimited) Priority-based scheduling policy: local-setting
VLAN Plan	Single VLAN tag: ● SVLAN ID: 1100 ● VLAN type: smart ● VLAN attribute: common ● UVLAN (upstream VLAN of the HGW): 43 ● CVLAN=UVLAN VLAN translation policy: ● ONU: transparently transmits the UVLAN of the HGW. ● OLT: implements VLAN translation: U<->S.

Procedure

Step 1 Configure the OLT.

1. Configure a traffic profile.

   Configure traffic profile 8. Set the CIR to off (unlimited), priority to 4, and priority-based scheduling policy to local-setting (that is, queues are scheduled based on the priority specified in the profile).

   NOTE

   Run the **display traffic table ip** command to query the existing traffic profiles in the system. If the existing traffic profiles in the system do not meet the requirements, run the **traffic table ip** command to add a traffic profile.

   ```
   huawei(config)#traffic table ip index 8 cir off priority 4 priority-policy
   local-setting
   ```

2. Configure the mapping relationship between a GEM port and a VDSL2 port on the ONU.

   The service flow of user VLAN 43 is mapped to GEM port 13 in the ONU line profile.

   ```
   huawei(config)#ont-lineprofile gpon profile-name fttd
   huawei(config-gpon-lineprofile-1)#gem mapping 13 4 vlan 43
   huawei(config-gpon-lineprofile-1)#commit
   huawei(config-gpon-lineprofile-1)#quit
   ```

3. Configure the VLAN of the Ethernet port on the ONU.

Copyright © Huawei Technologies Co., Ltd.

If the ONU is connected to the HGW through VDSL2 port 1, add VDSL2 port 1 to VLAN 43.

```
huawei(config)#ont-srvprofile gpon profile-name fttd
huawei(config-gpon-srvprofile-1)#port vlan vdsl 1 43
huawei(config-gpon-srvprofile-1)#commit
huawei(config-gpon-srvprofile-1)#quit
```

4. Create a service VLAN and add an upstream port to it.

   Add upstream port 0/19/0 to VLAN 1100.

   ```
   huawei(config)#vlan 1100 smart
   huawei(config)#port vlan 1100 0/19 0
   ```

5. Create service flows.

   Set the service VLAN to 1100, GEM port ID to 13, and user VLAN to 43, and use traffic profile 8.

   ```
   huawei(config)#service-port 3 vlan 1100 gpon 0/1/0 ont 1 gemport 13
   multi-service user-vlan 43 rx-cttr 8 tx-cttr 8
   ```

6. Save the data.

   ```
   huawei(config)#save
   ```

Step 2 Configure the HGW.

1. Log in to the web configuration window.

   a. Enter http://192.168.1.1/cu.html (default IP address) to the address bar of the IE browser and press **Enter**.

   b. In the login dialog box, enter the user name and password of the administrator (the Internet service provider (ISP) provides the default user name and default password). Then, click **OK**.

2. Set parameters for the VoD service.

   This example assumes LAN4 as an VoD port.

   a. Choose **Network** > **Bandwidth Configuration** from the navigation tree.

   b. In the right pane, create LAN connection 4 for the VoD service. Set the parameters as follows:

Parameter	Value
Bearing service	**OTHER**: The connection is used for the VoD service.
VLAN enabling	**Enable** VLAN tags are added to upstream packets. **NOTE** When VoD service flows are created on the OLT, the value is **Disable** if **uservlan** is untagged and the value is **Enable** if **uservlan** is tagged.
VLANID [1-4094]	VLAN ID corresponding to the user VLAN value for VoD service flows created on the OLT. In this example, set this parameter to 43.
Binding item	LAN4
Mode	Bridge

Copyright © Huawei Technologies Co., Ltd.

Parameter	Value
DHCP transparent transmission	Enable

c. Click **OK** to save the settings.

3. Restart the HGW.
   Choose **Management** > **Device Management** and click **Restarting the Device**.

----End

10.6.2.9 Verifying Services

In the FTTD scenario, ONUs are installed in users' houses which are far away from the central equipment room. ONUs provide remote service verification methods including PPPoE dialup emulation, and multicast emulation to facilitate configuration and commissioning engineers to verify services remotely after service configuration.

Prerequisites

ONUs and upper-layer devices have been connected properly. The BRAS and MGC/IMS have been configured.

Background

Remote Service Verification Method	Function	Description
PPPoE dialup emulation	An ONU simulates a PPPoE user terminal software to perform dialup and interact with the BRAS to verify the connectivity between the ONU and BRAS.	● PPPoE dialup emulation requires a service flow which does not belong to a QinQ VLAN. ● A user name, password, and authentication mode must be configured on the BRAS for the PPPoE dialup emulation. ● An ONU supports a maximum of a PPPoE dialup emulation.
Multicast emulation	This function enables you to simulate a multicast user going online and lead the program stream to an ONU. You can check whether the multicast service is normal by checking the real-time traffic of the multicast program.	Multicast services configured in the dynamic controllable multicast mode do not support this function.

Copyright © Huawei Technologies Co., Ltd.

Data plan

Item	Data	Remarks
PPPoE dialup emulation parameters	PPPoE user name: test@huawei Password: test	The user name, password, and authentication mode for the emulation test must be configured on the BRAS. The entered user name, password, and authentication mode must be consistent with those configured on the BRAS.
Multicast emulation parameters	Multicast service flow ID: 1 MVLAN: 1000 IP address of the multicast program: 224.1.1.10	-

Procedure

- Verify the Internet access service using PPPoE dialup emulation.
  1. In the xPON board mode, run the **pppoe simulate start** command to start a PPPoE dialup emulation test. The following test uses GPON as an example:

```
huawei(config)#interface gpon 0/1
huawei(config-if-gpon-0/1)#pppoe simulate start
{ portid<U><0,7> }:0
{ ontid<U><0,127> }:1
{ eth<K>|untagged<K>|vdsl|vlanid<U><0,4095> }:vdsl
{ ont-portid<U><1,8> }:1
{ untagged<K>|vlanid<U><0,4095> }:100
{ priority<U><0,7>|user-name<K> }:user-name
{ username<S><Length 1-64> }:test@huawei
{ user-password<K> }:user-password
{ password<S><Length 1-64> }:test
{ authentication-mode<K> }:authentication-mode
{ protocol<E><chap,pap> }:chap

  Command:
          pppoe simulate start 0 1 vdsl 1 100 user-name test@huawei user-
password
 test authentication-mode chap

huawei(config-if-gpon-0/1)#
  ---------------------------------
  ONT PPPoE Test Result
  ---------------------------------
  F/S/P                : 0/1/0
  ONT-ID               : 1
  ONT VDSL Port ID     : 1
  ONT Vlan ID          : 100
  Vlan Priority        : -
  Emluator result      : Success
   ---------------------------------
```

- Troubleshooting methods for the Internet access service
  1. Check whether configurations are complete on the OLT.
     - Run the **display ont info** command to query the ONU status to check whether the ONU is registered successfully.

Copyright © Huawei Technologies Co., Ltd.

- Run the **display service-port** command to check whether the Internet access service flow is configured and whether the inner VLAN ID of the service flow is consistent with that in the data plan.
- If a native VLAN is configured for the VDSL2 port on the ONU, run the **display ont port attribute** command in the xPON board mode to check whether the native VLAN is correct.

2. Check the upstream and downstream ports by checking the MAC address learning status.
   a. Run the **display mac-address vlan** command to check the MAC address learning status of the Internet service VLAN.
      - If the upstream port does not learn a MAC address, check the network connections between the upstream port and upper-layer devices and check the configurations of upper-layer devices.
      - If the downstream port does not learn a MAC address, check whether the ONU is activated, whether the PC is connected to the right port on the ONU, and whether the PC is working properly.
   b. Run the **display ont-learned-mac** command to check whether the ONU connecting to the PON port learned any MAC addresses.

      If not, check whether the ONU properly connects to the PC or home gateway (HGW).

- Verify the multicast service using multicast emulation.
  1. Run the **igmp static-join** command to simulate a multicast user to order a multicast program.

```
huawei(config)#btv
huawei(config-btv)#igmp static-join service-port 1 ip 224.1.1.10 vlan 1000
```

  NOTE

  If the multicast program is obtained dynamically, **igmp static-join** can be executed successfully only when the range for obtaining the dynamic program is set.

  2. Run the **display igmp user** command to query the status of the multicast user.

```
huawei(config-btv)#display igmp user service-port 1
  User                        : 0/1/0/1
  State                       : online
  Authentication              : no-auth
  Quick leave                 : MAC-based
  IGMP flow ID                : 1
  Video flow ID               : 1
  Log switch                  : enable
  Bind profiles               : -
  IGMP version                : IGMP v3
  Current version             : IGMP v3
  Current IGMP IPv6 version   : IGMP IPv6 v2
  Available programs          : 8
  Global leave                : disable
  User max bandwidth          : no-limit
  Used bandwidth(kbps)        : 0
  Used bandwidth
  to max bandwidth(%)         : -
  Total video bandwidth       : -
  Mcast video bandwidth       : -
  Active program list

------------------------------------------------------------------------
--
  Program name     VLAN  IP/MAC           State           Start time
```


Copyright © Huawei Technologies Co., Ltd.

```
------------------------------------------------------------------------
--
  PROGRAM-5        1000  224.1.1.10       watching        2011-10-29
                                                          16:33:41+08:00

------------------------------------------------------------------------
--
  Total: 1
```

3. Run the **display multicast flow-statistic** command to query the real-time traffic of the multicast program.

```
huawei(config-btv)#display multicast flow-statistic vlan 1000 ip
224.1.1.10
{ <cr>|sourceip<K> }:

  Command:
          display multicast flow-statistic vlan 1000 ip 224.1.1.10
  Command is being executed. Please wait...
  Multicast flow statistic result: 8736(kbps)
```

----End

Copyright © Huawei Technologies Co., Ltd.

11 FTTB and FTTC Solution Configuration

About This Chapter

The FTTB and FTTC solution configuration guide describes how to configure typical FTTB/C services (such as high-speed Internet access, multicast, and VoIP) on the OLT and the ONU step by step through examples.

11.1 FTTB and FTTC Service Overview
This topic describes FTTB and FTTC services from basic concepts, network scenarios, typical configurations, and ONU capability sets to provide necessary background information for FTTB and FTTC service configuration in different scenarios.

11.2 Principle of FTTB and FTTC Data Plan
This topic describes principles of data plan for various FTTB and FTTC networking diagrams in terms of device management, QoS, services, and security. The examples in this topic are based on these principles to plan data.

11.3 Configuring Services in Various FTTB and FTTC Scenarios (GPON and 10G GPON Access)
This topic describes how to configure the Internet access service, voice service and multicast service in GPON/10G GPON access mode in FTTB/FTTC networking scenarios.

11.4 Configuring Services in Various FTTB and FTTC Scenarios (Ethernet Cascading)
This section describes how to configure services when a multi-dwelling unit (MDU) serving as an independent node or GE remote extended subrack cascades with an optical line terminal (OLT)through Ethernet port.

Copyright © Huawei Technologies Co., Ltd.

11.1 FTTB and FTTC Service Overview

This topic describes FTTB and FTTC services from basic concepts, network scenarios, typical configurations, and ONU capability sets to provide necessary background information for FTTB and FTTC service configuration in different scenarios.

11.1.1 Basic Concept

FTTB and FTTC solutions involve many concepts. This topic describes concepts involved in FTTB and FTTC solutions from user side to network side based on the following integrated FTTB and FTTC network diagram.

Integrated FTTB and FTTC Network Diagram

Figure 11-1 Integrated FTTB and FTTC network diagram (PON)

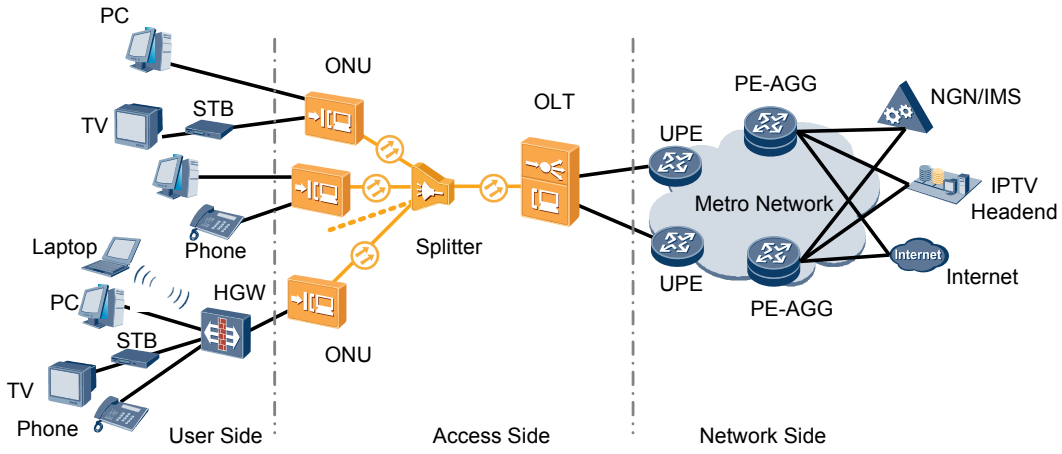
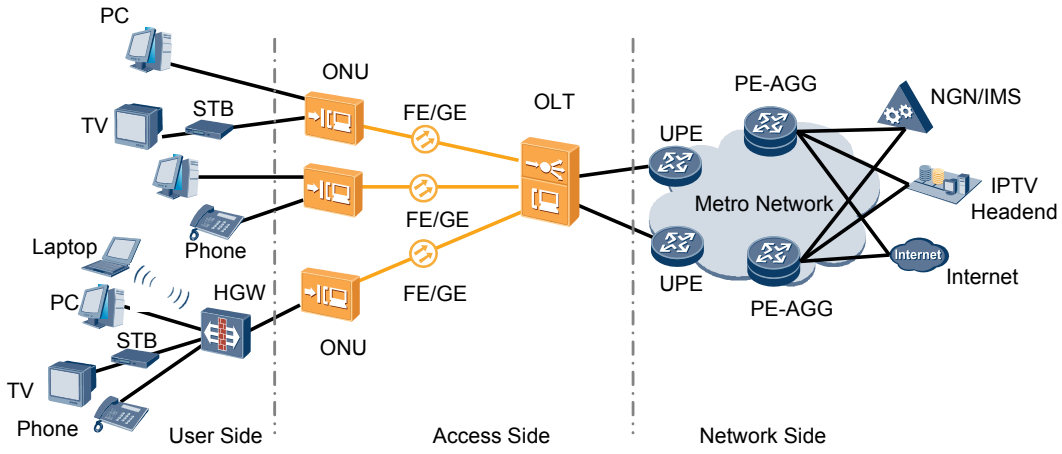


Figure 11-2 Integrated FTTB and FTTC network diagram (Ethernet cascading)



Copyright © Huawei Technologies Co., Ltd.

User Side

Concept	Introduction
HGW (or HG)	Home gateways (HGWs or HGs) are gateway devices designed for households and small-office network users. They provide routing functions, support various service interfaces (POTS, LAN, WLAN, or xDSL interfaces), and support remote management and diagnosis.
VoD	Video on demand (VoD) is known as interactive video on demand. Users can choose their desired programs from the VoD program database. When watching programs, users can perform operations such as pause, fast forward, fast rewind, and locate.
Multicast	Multicast, or broadband TV (BTV) is similar to traditional wired broadcasting or television satellite broadcasting. Users have the same experience in watching BTV programs and traditional television programs. Unlike the traditional television, the IPTV system encodes audio signals into media streams and multicasts the media streams over an IP network to user terminals.

Access Side

Concept	Introduction
PON	A passive optical network (PON) uses a point-to-multipoint (P2MP) network architecture. A PON network consists of three parts: optical line terminal (OLT), optical distribution network (ODN), and optical network units (ONUs). A PON network uses optical fibers for data transmission, supports more users with less optical fiber resources, and provides a higher access rate. Mainstream PON technologies include broadband passive optical network (BPON), Ethernet passive optical network (EPON), and gigabit passive optical network (GPON).
ODN	The ODN is composed of passive optical components, such as optical fibers and one or more passive optical splitters. The ODN provides highly reliable optical channels between the OLT and ONUs.
OLT	The OLT is an aggregation device located at the central office (CO), which terminates PON protocols. OLTs in this document are MA5600T/MA5603T/MA5608T.
ONU	ONUs are located on the user side, providing various types of ports for connecting to user terminals. The ONUs communicate with the OLT through a passive ODN. **NOTE** ONUs in FTTB and FTTC networks refer to multi-dwelling units (MDUs).

Copyright © Huawei Technologies Co., Ltd.

Concept	Introduction
Split Ratio	Split ratio is the ratio of dividing a downstream optical signal into subsignals in the PON system. Greater optical ratio requires more power to support physical distances.
PTP Ethernet cascading	On a point to point (P2P) Ethernet cascading network, the OLT uses P2P Ethernet access board and optical terminal to provide FTTx access to subscribers. The OLT can provide the combined service of video, voice, and data to meet application requirements of next-generation access devices.
FTTB	Fiber to the building (FTTB) applies to medium- and high-density apartments or office buildings. The OLT is connected to the ONU (deployed in the corridor) through optical fibers, and the ONU is then connected to users through twisted pairs to provide users with the voice, data, and video services.
FTTC	Fiber to the curb (FTTC) applies to scattered apartments and industrial parks. The OLT is connected to the ONU (deployed in the hole at the curb or FAT on a telegraph pole) through optical fibers, and the ONU is then connected to users through twisted pairs to provide users with the voice, data, and video services. **NOTE** The difference between FTTB and FTTC is the ONU position. To simply description, this document uses FTTB and FTTC, indicating that both FTTB and FTTC networks are supported.

Network Side

Concept	Introduction
U-PE	User-end provider edges (U-PEs) are routing devices directly connected to customer edges (UEs). U-PEs support routing and MPLS encapsulation. If a U-PE is connected to multiple CEs and possesses the basic bridging function, data frame forwarding only needs to be performed on the U-PE. This reduces the load of the S-PE.
PE-AGG	Aggregation provider edge (PE-AGG) routers provide aggregation and route forwarding functions for access equipment. Compared with U-PEs, PE-AGGs features higher performance, fewer interfaces, and higher switching rates.
NGN/IMS	A next generation network (NGN) is a network that uses softswitches as its core and uses open and standardized architectures to provide abundant services such as VoIP, video, and data. The IP multimedia subsystem (IMS) uses SIP signaling as its call control signaling to provide services such as VoIP, data, and multimedia services. **NOTE** NGN/IMS in this document refers to softswitches that support H.248 and SIP.

Copyright © Huawei Technologies Co., Ltd.

Concept	Introduction
IPTV Headend	The IPTV headend system functions as the contents preparation platform in the IPTV system. It provides functions such as signal receipt, media format conversion, and media material management.

11.1.2 Scenario and Hardware Configuration (GPON)

The typical GPON FTTB and FTTC networking scenarios and their OLT and ONU hardware configurations are listed in the table below.

Scenario	Description	OLT Typical Configuration (Main Control Board + Service Board +Upstream Board)	MDU Configuration
FTTB Networking (LAN Access Without HGW)	● The ONU is deployed in the building and is connected to the user's home through the category-5 cable. ● The ONU provides FE and POTS ports for the Internet access and VoIP services.	SCUN/SCUH+GPBD +GICF/GICG/X2CA	ONUs applicable to this scenario: MA5616, MA5822, MA5612
FTTB/ FTTC Networking (xDSL Access Without HGW)	● The ONU is deployed in the building or street fiber distribution terminal and is connected to the user's home through the twisted pair cable. ● The ONU provides xDSL and POTS ports for the Internet access and VoIP services.		ONUs applicable to this scenario: MA5616, MA5622A, MA5603T

Copyright © Huawei Technologies Co., Ltd.

Scenario	Description	OLT Typical Configuration (Main Control Board + Service Board +Upstream Board)	MDU Configuration
FTTB/ FTTC +HGW Networking (ONU Providing the VoIP Service)	● The ONU is deployed in the building or street fiber distribution terminal and uses LAN or xDSL to connect to the HGW deployed at user's home. The HGW provides service access interfaces and the built-in IAD of the ONU provides the VoIP service. ● The HGW provides the Internet access and IPTV services by connecting to the upstream ONU using LAN or xDSL.		ONUs applicable to this scenario: MA5822, MA5616, MA5622A, MA5603T, MA5612. Among these ONUs: ● ONUs with LAN ports include MA5616, MA5822, MA5612. ● ONUs with xDSL ports include MA5616, MA5622A, MA5603T.

Copyright © Huawei Technologies Co., Ltd.

Scenario	Description	OLT Typical Configuration (Main Control Board + Service Board +Upstream Board)	MDU Configuration
FTTB/ FTTC +HGW Networking (HGW Providing the VoIP Service)	● The ONU is deployed in the building or street fiber distribution terminal and uses LAN or xDSL to connect to the HGW deployed at user's home. ● The HGW provides the Internet access, IPTV, and VoIP services by connecting to the upstream ONU using LAN or xDSL. The built-in IAD of the HGW provides the VoIP service.		ONUs applicable to this scenario: MA5616, MA5821, MA5822, MA5622A, MA5623, MA5623A, MA5611S-AE16, MA5611S-AE16 (No SPL), MA5611S-DE16, MA5611S-DE48 (900-ohm impedance), MA5611S-DE48, MA5611S-DE48-A, MA5603T, MA5612, MA5612A. Among these ONUs: ● ONUs with LAN ports include MA5616, MA5821, MA5612, MA5612A. ● ONUs with ADSL2+ ports include MA5616, MA5603T. ● ONUs with VDSL2 ports include MA5616, MA5622A, MA5623, MA5623A, MA5611S-AE16, MA5611S-AE16 (No SPL), MA5611S-DE16, MA5611S-DE48 (900-ohm impedance), MA5611S-DE48,

Copyright © Huawei Technologies Co., Ltd.

Scenario	Description	OLT Typical Configuration (Main Control Board + Service Board +Upstream Board)	MDU Configuration
			MA5611S-DE48-A, MA5603T.

11.1.3 Scenario and Hardware Configuration (10G GPON)

The typical 10G GPON FTTB and FTTC networking scenarios and their OLT and ONU hardware configurations are listed in the table below.

Scenario	Description	MDU Configuration
FTTB Networking (LAN Access Without HGW)	● The ONU is deployed in the building and is connected to the user's home through the category-5 cable. ● The ONU provides FE and POTS ports for the Internet access and VoIP services.	ONUs applicable to this scenario: ● MA5616 ● MA5822
FTTB/C Networking (xDSL Access Without HGW)	● The ONU is deployed in the building or street fiber distribution terminal and is connected to the user's home through the twisted pair cable. ● The ONU provides xDSL and POTS ports for the Internet access and VoIP services.	ONUs applicable to this scenario: MA5616
FTTB/C+HGW Networking (ONU Providing the VoIP Service)	● The ONU is deployed in the building or street fiber distribution terminal and uses LAN or xDSL to connect to the HGW deployed at user's home. The HGW provides service access interfaces and the built-in IAD of the ONU provides the VoIP service. ● The HGW provides the Internet access and IPTV services by connecting to the upstream ONU using LAN or xDSL.	ONUs applicable to this scenario: ● MA5616 ● MA5822

Copyright © Huawei Technologies Co., Ltd.

Scenario	Description	MDU Configuration
FTTB/C+HGW Networking (HGW Providing the VoIP Service)	● The ONU is deployed in the building or street fiber distribution terminal and uses LAN or xDSL to connect to the HGW placed at user's home. ● The HGW provides the Internet access, IPTV, and VoIP services by connecting to the upstream ONU using LAN or xDSL. The built-in IAD of the HGW provides the VoIP service.	ONUs applicable to this scenario: ● MA5616 ● MA5821

11.1.4 Networking Scenarios and Hardware Configurations (Ethernet Cascading)

This section describes the typical fiber to the building (FTTB) or fiber to the curb (FTTC) Ethernet cascading networks and typical hardware configurations of the access devices on the networks.

- On an Ethernet cascading network, users connect to the network through xDSL lines. An optical network unit (ONU) using GE upstream transmission is used as a digital subscriber line access multiplexer (DSLAM) and connects to a device on the metropolitan area network (MAN). This is the mainstream networking of carriers. The data plan, configuration, and maintenance of the ONU are the same as those of the existing DSLAMs on live networks and therefore are not described in this section.
- The recommended networking is as follows: ONU using GE upstream transmission -> optical line terminal (OLT) -> MAN device. This is an FTTB or FTTC Ethernet cascading network. The network of this type reduces optical fibers and operating expense (OPEX) of carriers through O&M functions, such as remote software commissioning using GE upstream transmission. An FTTB or FTTC Ethernet cascading network is available in one of the following types:
  - Independent NE networking: An ONU has a separate management IP address. The operations support system (OSS) and U2000 manage the ONU as an independent NE.
  - GE remote extended subrack networking in centralized management mode: An ONU does not have a management IP address. Instead, it is managed as a GE remote extended subrack (extended subrack for short) of the OLT (master subrack). The ONU is regarded as a remote service board of the OLT. The network of this type applies if more users need to be covered without increasing the number of NEs on the network. The GE remote extended subrack networking reduces the OPEX and total cost of operation (TCO) of carriers.

Copyright © Huawei Technologies Co., Ltd.

Networking Scenario	Description	Typical OLT or Master Subrack Configuration	ONU or Extended Subrack Device
FTTB and FTTC Ethernet Cascade Networking (ONU works as an independent NE)	● ONUs are deployed in corridors or fiber distribution terminals (FDTs) on the curb. They connected to users through twisted pairs. ● The networking between the ONU and users is the same as the xDSL networking for a PON network. The networking applies in the following scenarios: – FTTB and FTTC networking in xDSL access mode, without a home gateway (HGW) – FTTB/FTTC+HGW networking (The voice service is provided through the ONU.) – FTTB/FTTC+HGW networking (The voice service is provided through the HGW.)	MA5600T or MA5603T: ● Control board: SCUN or SCUH ● Service board: OPGD or ETHB ● Upstream interface board: GICF, GICG, X1CA, or X2CA	ONU series supporting GE upstream transmission. For details, see **11.1.7 Ethernet Upstream ONU Capability Sets**.
FTTB and FTTC Ethernet Cascade Networking (ONU works as a GE remote extended subrack)	● Extended subracks are deployed in corridors or FDTs on the curb. They connected to users through twisted pairs. ● The networking applies to high-bandwidth access scenarios and provides the high-speed Internet access service, voice service, and IPTV service. In the scenarios, an HGW is configured on the user side and VDSL2 is used for downstream transmission.	MA5600T or MA5603T: ● Control board: SCUN ● Service board: ETHB ● Upstream interface board: GICF, GICG, X1CA, or X2CA	MA5623AR

Copyright © Huawei Technologies Co., Ltd.

11.1.5 GPON ONU Capability Sets

This topic describes the hardware capabilities and usage scenarios of GPON optical network units (ONUs) on fiber to the building (FTTB) or fiber to the curb (FTTC) networks.

Table 11-1 shows the GPON ONU capability sets provided by Huawei.

NOTE

The **Service Port** column in **Table 11-1** lists only service ports supported by all configurations of an ONU type. For details about ONU configuration, see the product document released for the related version.

The **Supported ONU Version** column in **Table 11-1** lists only ONU versions supported by FTTx V100R006 and later.

Table 11-1 GPON ONU capability sets

ONU Type	Service Port	Supported ONU Version	Usage Scenarios
MA5620	● FE electrical ports ● POTS ports	● V800R308C00 ● V800R310C00 ● V800R312C01	The MA5620 applies to FTTB scenarios.
MA5626	● FE electrical ports ● GE electrical ports (PoE)	V800R308C00	The MA5626 applies to FTTB scenarios.
	● FE electrical ports (PoE) ● GE electrical ports (PoE)	V800R308C01	
	● FE electrical ports ● GE electrical ports (PoE) ● FE electrical ports (reverse PoE)	V800R310C00	
	● FE electrical ports ● FE electrical ports (reverse PoE)	V800R312C01	
MA5622A	● VDSL2 ports (Supports vectoring) ● POTS ports	● V800R311C00 ● V800R313C00 ● V800R015C00	The MA5622A, MA5623, and MA5623A apply to FTTB and FTTC scenarios.
MA5623	VDSL2 ports	● V800R311C00 ● V800R313C00	

Copyright © Huawei Technologies Co., Ltd.

ONU Type	Service Port	Supported ONU Version	Usage Scenarios
MA5623A	VDSL2 ports (Supports vectoring)	● V800R311C01 ● V800R312C00 ● V800R313C00 ● V800R313C10	
MA5612	● GE electrical ports ● FE electrical ports ● POTS ports ● E1 or T1 ports ● RF ports (optional)	● V800R308C00 ● V800R308C01 ● V800R310C00 ● V800R311C00 ● V800R312C00 ● V800R015C00	The MA5612 and MA5612A apply to FTTB scenarios. In addition, the MA5612 applies to private line access scenarios.
MA5612A	● GE electrical ports ● FE electrical ports	● V800R308C00 ● V800R310C00 ● V800R312C00 ● V800R015C00	

Copyright © Huawei Technologies Co., Ltd.

ONU Type	Service Port	Supported ONU Version	Usage Scenarios
MA5616 (CCUB control board)	● ADSL2+ ports ● VDSL2 ports ● SHDSL ports ● POTS ports ● ISDN ports	● V800R308C01 ● V800R309C00 ● V800R310C00 ● V800R311C00 ● V800R312C00 ● V800R313C00 ● V800R015C00	The MA5616 applies to FTTB and FTTC scenarios.
MA5616 (CCUC control board)	● FE optical ports ● GE optical ports ● GE electrical ports ● ADSL2+ ports ● VDSL2 ports ● SHDSL ports ● POTS ports ● ISDN ports	● V800R308C02 ● V800R309C00 ● V800R310C00 ● V800R311C00 ● V800R312C00 ● V800R313C00 ● V800R015C00	
MA5616 (CCUE control board)	● FE optical ports ● GE optical ports ● GE electrical ports ● ADSL2+ ports ● VDSL2 ports (Supports vectoring) ● SHDSL ports ● POTS ports ● ISDN ports	● V800R311C01 ● V800R312C00 ● V800R313C00 ● V800R015C00	

Copyright © Huawei Technologies Co., Ltd.

ONU Type	Service Port	Supported ONU Version	Usage Scenarios
MA5616 (CCUD control board)	● FE optical ports ● GE optical ports ● GE electrical ports ● ADSL2+ ports ● VDSL2 ports ● SHDSL ports ● POTS ports ● ISDN ports	● V800R312C00 ● V800R313C00 ● V800R015C00	
MA5652	● VDSL2 ports ● RF ports	V800R310C00	The MA5652 applies to FTTB and FTTC scenarios.
MA5662	VDSL2 ports	● V800R309C00 ● V800R310C00	The MA5662 applies to FTTB and FTTC scenarios.
MA5611S-AE16	VDSL2 ports (Supports vectoring)	● V800R313C00 ● V800R015C00	The MA5611S applies to FTTB and FTTC scenarios.
MA5611S-AE16 (No SPL)	VDSL2 ports (Supports vectoring)	V800R015C00	The MA5611S applies to FTTB and FTTC scenarios.
MA5611S-DE16	VDSL2 ports (Supports vectoring)	V800R015C00	The MA5611S applies to FTTB and FTTC scenarios.
MA5611S-DE48 (900-ohm impedance)	VDSL2 ports (Supports vectoring)	V800R015C00	The MA5611S applies to FTTB and FTTC scenarios.
MA5611S-DE48	VDSL2 ports (Supports vectoring)	V800R015C00	The MA5611S applies to FTTB and FTTC scenarios.

Copyright © Huawei Technologies Co., Ltd.

ONU Type	Service Port	Supported ONU Version	Usage Scenarios
MA5611S-DE48-A	VDSL2 ports (Supports vectoring)	V800R015C00	The MA5611S applies to FTTB and FTTC scenarios.
MA5821 or MA5822	● MA5821: FE electrical ports ● MA5822: FE electrical ports, and POTS ports	V800R313C00	The MA5821 and MA5822 apply to FTTB and FTTC scenarios.
MA5603T	● ADSL2+ ports ● VDSL2 ports (Supports vectoring since V800R011) ● SHDSL ports ● POTS ports ● ISDN ports	● V800R008C01 ● V800R011C00 ● V800R012C00 ● V800R013C00 ● V800R015C00	The MA5603T applies to FTTB and FTTC scenarios, especially to FTTC scenarios.

11.1.6 10G GPON ONU Capability Sets

This topic describes the hardware capabilities, features, and positioning of 10G GPON ONUs in FTTB and FTTC networks.

Table 11-2 shows the 10G GPON ONU capability sets provided.

Table 11-2 10G GPON ONU capability sets

ONU Type	User Port	ONU Version Supported	Positioning
MA5821	The MA5821 has the following specifications: ● 1: 8 FE electrical ports ● 2: 16 FE electrical ports ● 3: 24 FE electrical ports	V800R313C00	It is mainly used on FTTB networks.

Copyright © Huawei Technologies Co., Ltd.

ONU Type	User Port	ONU Version Supported	Positioning
MA5822	The MA5822 has the following specifications: ● 1: 8 FE electrical ports + 8 POTS ports ● 2: 16 FE electrical ports + 16 POTS ports ● 3: 24 FE electrical ports + 24 POTS ports	V800R313C00	It is mainly used on FTTB networks.
MA5616 (CCUE control board)	The MA5616 has the following specifications: ● Ethernet access board: EIUD, EIUA ● ADSL2 service boards: ADLE and ADPE ● ADSL2+ + POTS combo service board: CALE ● VDSL2 service boards: VDGE, VDSH, VDTH, VDSE, VDLE, and VDLF ● VDSL2 + POTS combo board: CVLC ● Voice service boards: ASRB and ASPB ● SHDSL service board: SHLH ● ISDN service board: DSLD	V800R313C00	It is mainly used in FTTB and FTTC networks.

11.1.7 Ethernet Upstream ONU Capability Sets

This topic describes the hardware capabilities and usage scenarios of optical network units (ONUs) for Ethernet upstream transmission on fiber to the building (FTTB) or fiber to the curb (FTTC) networks.

Table 11-3 shows the Ethernet upstream ONU capability sets provided by Huawei.

NOTE

The **Service Port** column in **Table 11-3** lists only service ports supported by all configurations of an ONU type. For details about ONU configuration, see the product document released for the related version.

The **Supported ONU Version** column in **Table 11-3** lists only ONU versions supported by FTTx V100R006 and later.

Copyright © Huawei Technologies Co., Ltd.

Table 11-3 Ethernet Upstream ONU capability sets

ONU Type	Service Port	Supported ONU Version	Usage Scenarios
MA5622A	● VDSL2 ports (Supports vectoring) ● POTS ports	● V800R311C00 ● V800R313C00 ● V800R015C00	The MA5622A, MA5623, and MA5623A apply to FTTB and FTTC scenarios.
MA5623	VDSL2 ports	● V800R311C00 ● V800R313C00	
MA5623A	VDSL2 ports (Supports vectoring)	● V800R311C01 ● V800R312C00 ● V800R313C00 ● V800R313C10	
MA5612	● GE electrical ports ● FE electrical ports ● POTS ports ● E1 or T1 ports ● RF ports (optional)	● V800R308C00 ● V800R308C01 ● V800R310C00 ● V800R311C00 ● V800R312C00 ● V800R015C00	The MA5612 and MA5612A apply to FTTB scenarios. In addition, the MA5612 applies to private line access scenarios.
MA5612A	● GE electrical ports ● FE electrical ports	● V800R308C00 ● V800R310C00 ● V800R312C00 ● V800R015C00	

Copyright © Huawei Technologies Co., Ltd.

ONU Type	Service Port	Supported ONU Version	Usage Scenarios
MA5616 (CCUB control board)	● ADSL2+ ports ● VDSL2 ports ● SHDSL ports ● POTS ports ● ISDN ports	● V800R308C01 ● V800R309C00 ● V800R310C00 ● V800R311C00 ● V800R312C00 ● V800R313C00 ● V800R015C00	The MA5616 applies to FTTB and FTTC scenarios.
MA5616 (CCUC control board)	● FE optical ports ● GE optical ports ● GE electrical ports ● ADSL2+ ports ● VDSL2 ports ● SHDSL ports ● POTS ports ● ISDN ports	● V800R308C02 ● V800R309C00 ● V800R310C00 ● V800R311C00 ● V800R312C00 ● V800R313C00 ● V800R015C00	
MA5616 (CCUE control board)	● FE optical ports ● GE optical ports ● GE electrical ports ● ADSL2+ ports ● VDSL2 ports (Supports vectoring) ● SHDSL ports ● POTS ports ● ISDN ports	● V800R311C01 ● V800R312C00 ● V800R313C00 ● V800R015C00	

Copyright © Huawei Technologies Co., Ltd.

ONU Type	Service Port	Supported ONU Version	Usage Scenarios
MA5616 (CCUD control board)	● FE optical ports ● GE optical ports ● GE electrical ports ● ADSL2+ ports ● VDSL2 ports ● SHDSL ports ● POTS ports ● ISDN ports	● V800R312C00 ● V800R313C00 ● V800R015C00	
MA5652	● VDSL2 ports ● RF ports	V800R310C00	The MA5652 applies to FTTB and FTTC scenarios.
MA5662	VDSL2 ports	● V800R309C00 ● V800R310C00	The MA5662 applies to FTTB and FTTC scenarios.
MA5611S-AE16	VDSL2 ports (Supports vectoring)	● V800R313C00 ● V800R015C00	The MA5611S applies to FTTB and FTTC scenarios.
MA5611S-AE16 (No SPL)	VDSL2 ports (Supports vectoring)	V800R015C00	The MA5611S applies to FTTB and FTTC scenarios.
MA5611S-DE16 (BT complex impedance)	VDSL2 ports (Supports vectoring)	V800R015C00	The MA5611S applies to FTTB and FTTC scenarios.
MA5611S-DE16	VDSL2 ports (Supports vectoring)	V800R015C00	The MA5611S applies to FTTB and FTTC scenarios.
MA5611S-DE48 (900-ohm impedance)	VDSL2 ports (Supports vectoring)	V800R015C00	The MA5611S applies to FTTB and FTTC scenarios.

Copyright © Huawei Technologies Co., Ltd.

ONU Type	Service Port	Supported ONU Version	Usage Scenarios
MA5611S-DE48	VDSL2 ports (Supports vectoring)	V800R015C00	The MA5611S applies to FTTB and FTTC scenarios.
MA5611S-DE48-A	VDSL2 ports (Supports vectoring)	V800R015C00	The MA5611S applies to FTTB and FTTC scenarios.
MA5611S-AE48	VDSL2 ports (Supports vectoring)	V800R015C00	The MA5611S applies to FTTB and FTTC scenarios.
MA5821 or MA5822	● MA5821: FE electrical ports ● MA5822: FE electrical ports, and POTS ports	V800R313C00	The MA5821 and MA5822 apply to FTTB and FTTC scenarios.
MA5603T	● ADSL2+ ports ● VDSL2 ports (Supports vectoring since V800R011) ● SHDSL ports ● POTS ports ● ISDN ports	● V800R008C01 ● V800R011C00 ● V800R012C00 ● V800R013C00 ● V800R015C00	The MA5603T applies to FTTB and FTTC scenarios, especially to FTTC scenarios.

11.2 Principle of FTTB and FTTC Data Plan

This topic describes principles of data plan for various FTTB and FTTC networking diagrams in terms of device management, QoS, services, and security. The examples in this topic are based on these principles to plan data.

11.2.1 Principle of Device Management Data Plan

The device management plan includes channel management plan and the IP address plan.

Copyright © Huawei Technologies Co., Ltd.

Plan	Device/Service	Introduction
Management channel	OLT	Use a single S-VLAN as the equipment management VLAN of the OLT and that of all other equipment in the network.
	ONU/MDU/GE remote extended subrack	Use a single S-VLAN as the equipment management VLAN of the ONU and that of all other equipment in the network.
	HGW	Use a single S-VLAN as the management VLAN of the HGW that are managed by the items. Set a management VLAN for an entire network, an OLT, a PON board, or a PON port for identifying services and physical locations. It is recommended that you set different HGW management VLANs for the OLTs connected to one SR to avoid an excessively large broadcast domain of the SR and convergence switch.
IP address plan	Device management	It is recommended that you use private network IP addresses as the management IP address of the OLT and MDU for securing network devices.
	Internet access service	A PC obtains a public network IP address using PPPoE dialup for Internet access. The HGW obtains a public network IP address using PPPoE dialup. A PC obtains a private network IP address using DHCP.
	VoIP service	If an MDU has a built-in voice module, the MDU functions as a DHCP client and obtains IP addresses using DHCP. Multiple POTS ports on the MDU share one public network IP address. If an HGW has a built-in voice module, the HGW obtains IP address using DHCP.
	IPTV service	An STB obtains a public network IP address using DHCP and the subscriber can order programs. The MDU is only used for transparent transmission.
	TR069 service	For scenarios in which TR069 is used for management, maintenance, and service provisioning, the HGW functions as a DHCP client, obtains a public network IP address using DHCP, and connects to the TR069 server (ACS).

Copyright © Huawei Technologies Co., Ltd.

11.2.2 Principle of QoS Data Plan

The QoS plan for FTTB is an E2E planning, and it can be divided into following policies: traffic classification, marking, scheduling, traffic monitoring, and DBA policies.

Traffic Classification, Marking, and Scheduling Policies

Service Type	802.1p Priority	Queue Scheduling Method	OLT Queue ID (8 Queues)	ONT Queue.ID	
				Supporting Eight Queues	Supporting Four Queues
Management service	6	PQ	6	6	3
VoIP service	5	PQ	5	5	2
IPTV service	4	PQ	4	4	2
Internet access service	0	PQ	0	0	0

Note

- Different service packets are distinguished by different VLAN IDs. GEM ports are mapped based on 802.1p priorities for the GPON system.
- Service priorities in this table are recommended values. The service priorities are arranged according to the operators's actual planning.

Traffic Monitoring and DBA Policies

Items	Management service	Internet access service	VoIP service	IPTV service
GEM port	11 [Remark 1]	12	13	14
TCONT	All services share a T-CONT.			
DBA type	Type 3 (DBA profile: assured bandwidth + maximum bandwidth. Users are allowed to preempt the bandwidth on condition that the users' assured bandwidth is guaranteed. However, the total bandwidth cannot exceed the maximum bandwidth.)			
DBA bandwidth planning	Configure the DBA bandwidth according to the user's bandwidth package. The assured bandwidth is the maximum bandwidth required by management packets, VoIP, and IPTV upstream packets. The maximum bandwidth is larger than or equal to the maximum bandwidth that users apply.			

Copyright © Huawei Technologies Co., Ltd.

Items	Management service	Internet access service	VoIP service	IPTV service
Rate limit on OLT downstream	No rate limit	Configure rate limit by a traffic profile as required. [Remark 2]	No rate limit	No rate limit
Rate limit on ONU upstream port	Set ONU port rate limit or xDSL line rate limit as required. [Remark 2]			
Rate limit on ONU downstream port	Set ONU port rate limit or xDSL line rate limit as required. [Remark 2]			

Remark 1: GEM port value depends on the planning of the service provider, but in principle, use different GEM ports for different services.

Remark 2: **Table 11-4** shows the reference service bandwidth of each service for each user.

Table 11-4 Reference Service Bandwidth of Each service for Each User

Service Type	Upstream Bandwidth	Downstream Bandwidth	Bandwidth Description
Internet access service	Determined based on the tariff package.	Determined based on the tariff package.	Available bandwidth of Internet access service = Committed bandwidth of the tariff package - VoIP bandwidth - IPTV bandwidth
VoIP service	200 kbit/s	200 kbit/s	The upstream bandwidth and the downstream bandwidth of VoIP service are symmetrical. The actual bandwidth varies with the coding format. This bandwidth is calculated for two POTS ports.
IPTV service (common program)	/	2.5 Mbit/schannel	IPTV service mainly occupies the downstream bandwidth. The actual bandwidth depends on the coding format, the picture in picture information, 10% bandwidth burst traffic, and the number of programs that can be concurrently watched by one user (in the case of multi STBs access). The upstream bandwidth is mainly used for

Copyright © Huawei Technologies Co., Ltd.

Service Type	Upstream Bandwidth	Downstream Bandwidth	Bandwidth Description
IPTV service (high definition program)	/	9.7 Mbit/s channel	transmitting IGMP packets, which requires little bandwidth and can be neglected.

Note

- Rate limit on the BRAS or SR is recommended. OLTs and ONUs do not limit rates on service flows. If the BRAS does not support rate limit, OLTs can limit rates on service flows using traffic profiles.
- Different service packets of ONUs are distinguished by 802.1p priorities and are mapped to GEM ports based on 802.1p priorities so that packets are transmitted to different GEM ports. Each GEM port (each service) corresponds to a T-CONT or all GEM ports share a T-CONT.
- The sum of assured bandwidth of all ONTs under a PON port and the fixed bandwidth of OMCI management channel is smaller than the GPON upstream bandwidth. Some bandwidth must be reserved for future service expansion.

11.2.3 Principle of Internet Access Service Data Plan

The Internet access service plan mainly includes the plan of the VLAN and VLAN translation policy in different network scenarios.

VLAN Planning and VLAN Translation Policy on PON Networks

Application Scenario	VLAN Plan	VLAN Translation	
		ONU	OLT
FTTB networking (without HGWs)	Two-tagged VLAN (S-VLAN +C-VLAN)	The inner C-VLAN is mapped based on user ports to ensure that ONUs under the same PON board do not have the same C-VLAN.	The OLT translates VLANs and adds an S-VLAN. C'-VLAN <-> S-VLAN + C-VLAN
FTTB/FTTC+HGW networking (ONU providing the VoIP service)		HGWs (LAN upstream transmission)	

Copyright © Huawei Technologies Co., Ltd.

Application Scenario	VLAN Plan	VLAN Translation	
		ONU	OLT
FTTB/FTTC+HGW networking (HGW providing the VoIP service)		● Untagged upstream packets of HGWs: ONUs map C-VLANs based on user ports. ● Tagged upstream packets of HGWs: ONUs translate user VLANs to C'-VLANs. [Remark 1] HGWs (xDSL upstream transmission): ONUs translate PVCs to C'-VLANs.	

Note

- To ensure traceability of users and finer-grained QoS control and management of users and services, plan per user per service per VLAN (PUPSPV) for the Internet access service. Considering OLT capacity and VLAN scalability, use dual VLANs (S-VLAN+C-VLAN) on the OLT to differentiate users for the Internet access service.
- The outer S-VLAN, which identifies services and physical location, can be allocated based on the OLT, PON board (recommended), or PON port (recommended). The inner C-VLAN identifies users. User C-VLANs are unique in one S-VLAN.

  NOTE

  It is recommended that you associate C-VLAN IDs with PON ports, optical splitters, and ONU ports to ensure C-VLAN uniqueness and to facilitate location. Example: C-VLAN ID = 256 x PON port ID + 32 x Split ratio x (Optical port ID - 1) + ONU port ID + 1
- It is recommended that you use stacking VLANs as S-VLANs so that security features, such as PPPoE+/option 82, and anti-MAC attack, and anti-MAC spoofing can be easily deployed.

Copyright © Huawei Technologies Co., Ltd.

VLAN Planning and VLAN Translation Policy on Ethernet Cascading Networks

Application Scenario	VLAN Plan	VLAN Translation	
		MDU/GE Remote Extended Subrack	OLT/ Master Subrack
FTTB and FTTC Ethernet cascading (MDUs serving as independent nodes)	Two-tag VLAN solution	Without HGWs: The outer S-VLAN is planned based on MDUs and the inner C-VLAN identifies a user. Ensure that the C-VLANs of users using the same S-VLAN do not repeat each other. LAN access using HGWs: ● Untagged upstream packets of HGWs: MDUs map C-VLANs based on user ports and add S-VLANs to packets. ● Tagged upstream packets of HGWs: MDUs translate user VLANs to C-VLANs (user VLAN <-> C-VLAN) and add S-VLANs to packets. xDSL access using HGWs: ● Asynchronous transfer mode (ATM) upstream transmission: MDUs translate PVCs to C-VLANs (PVC <-> C-VLAN) and add S-VLANs to packets. Ensure that the C-VLANs of users using the same S-VLAN do not repeat each other. ● Packet transfer mode (PTM) upstream transmission: Untagged upstream packets of HGWs: MDUs map C-VLANs based on user ports and add S-VLANs to packets. Tagged upstream packets of HGWs: MDUs translate user VLANs to C-VLANs (user VLAN <-> C-VLAN) and add S-VLANs to packets. Ensure that the C-VLANs of users using the same S-VLAN do not repeat each other.	The OLT transmits packets transparently.

Copyright © Huawei Technologies Co., Ltd.

Application Scenario	VLAN Plan	VLAN Translation	
		MDU/GE Remote Extended Subrack	OLT/ Master Subrack
FTTB and FTTC Ethernet cascading (centralized management for GE remote extended subracks)		● Without HGWs: The extended subrack maps inner C-VLANs based on user ports and adds S-VLANs to packets. Ensure that the C-VLANs of users using the same S-VLAN do not repeat each other. ● xDSL access using HGWs: – ATM upstream transmission: The extended subrack translates PVCs to C-VLANs (PVC <-> C-VLAN) and adds S-VLANs to packets. Ensure that the C-VLANs of users using the same S-VLAN do not repeat each other. – PTM upstream transmission: Untagged upstream packets of HGWs: The extended subrack maps C-VLANs based on user ports and adds S-VLANs to packets. User-VLAN-tagged upstream packets of HGWs: The extended subrack translates user VLANs to C-VLANs (user VLAN <-> C-VLAN) and adds S-VLANs to packets. Ensure that the C-VLANs of users using the same S-VLAN do not repeat each other.	The master subrack transmits packets transparently.

11.2.4 (Optional) Principle of Vectoring Data Plan

Vectoring data plan includes grouping, the policy for activating a legacy customer premises equipment (CPE), and line profile planning of a port.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
Grouping	In vectoring network planning, grouping is a key phase. Accurate grouping cancels inter-line crosstalk to the largest extent and develops vectoring advantages. ● It is recommended that you learn the actual physical routing beforehand. Crosstalk between lines in a bundle reaches the maximum value. Therefore, it is better to plan members in a vectoring group the same as actual routing. ● If you do not know actual routing in the system, you cannot group. In this case, you can use the default global grouping. Then, you can add all lines supporting vectoring to default vectoring group 1.
Policy for activating a legacy customer premises equipment (CPE)	A legacy CPE is a VDSL2 CPE that supports G.993.2 but does not support G.9930.5 or vectoring. If such a CPE is activated by G. 993.2 in the vectoring system, it affects lines and the performance of the vectoring system deteriorates. Therefore, configure the policy for activating a vectoring legacy CPE based on site requirements to reduce the effect to minimum. The system supports three activation polices. The default policy is **limit**. ● No-limit: The legacy CPE can be activated in the common VDSL2 mode. That is, the legacy CPE is activated in the non-Vectoring mode and the performance of the Vectoring system is affected. This activation policy is generally used in the initial stage of Vectoring applications. In this stage, a lot of CPEs need to be upgraded or replaced and the Vectoring performance is not mostly concerned. ● Limit: The legacy CPE can be activated in the common VDSL2 mode; however, the line is automatically shaped by power spectrum density (PSD) and is activated by low-speed VDSL2 to prevent other lines from being affected. This activation policy is generally used in the medium stage of Vectoring applications. In this stage, some CPEs are not upgraded or replaced. This is the system default policy. ● Force-friendly-ds-limit-us: **force friendly** is used in the downstream direction and PSD automatic shaping is used in the upstream direction. ● Force-friendly-ds-no-limit-us: **force friendly** is used in the downstream direction and no restriction is used in the upstream direction. ● Block: The legacy CPE cannot be activated in the common VDSL2 mode (G.993.2). If a legacy CPE needs to be activated in G.993.2 mode, you need to delete it from the Vectoring group first. This activation policy is generally used in the mature stage of Vectoring applications. In this stage, the Vectoring performance is concerned and unnecessary crosstalk is better to be masked.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
Line profile of a port	The maximum rate in the line profile bound to a port is the target value for vectoring rate improvement. Carriers need to plan the line profile based on services.

11.2.5 Principle of VoIP Service Data Plan

The VoIP service plan mainly includes the plan of VLANs and VLAN translation policy in different network scenarios, and the plan of voice protocols.

VLAN Planning and VLAN Translation Policy on PON Networks

Application Scenario	VLAN Plan	VLAN Translation		Remarks
		ONU	OLT	
FTTB networking (without HGWs)	Single-tagged VLAN	ONUs provide the VoIP service and use the same S-VLAN.	Transparently transmits packets.	-
FTTB+HGW networking (ONU providing the VoIP service)	Single-tagged VLAN	ONUs provide the VoIP service and use the same S-VLAN.	Transparently transmits packets.	This solution is recommended.
	Double-tagged VLAN (S-VLAN+C-VLAN)	ONUs provide the VoIP service and use the same C-VLAN.	The OLT adds one S-VLAN tag: C-VLAN <-> S-VLAN+C-VLAN.	This solution is used only when double-tagged VLANs are planned.
FTTB+HGW networking (HGW providing the VoIP service)	Single-tagged VLAN	When packets sent from the HGW using LAN upstream transmission carries user VLANs, the ONU translates user VLANs to C-VLANs. HGWs (xDSL upstream transmission): ONUs translate PVCs to C'-VLANs.	Transparently transmits packets.	This solution is recommended.
	Double-tagged VLAN (S-VLAN+C-VLAN)		The OLT adds one S-VLAN tag: C-VLAN <-> S-VLAN+C-VLAN.	This solution is used only when double-tagged VLANs are planned.

Copyright © Huawei Technologies Co., Ltd.

Note

- The VoIP service is a closed service self-operated by carriers. The single-tagged S-VLAN is the mainstream application and is recommended.
- Set an S-VLAN for an entire network, an OLT, a PON board, or a PON port for identifying services and physical locations. It is recommended that you set different VoIP VLANs for the OLTs connected to one VoIP SR to avoid an excessively large broadcast domain of the VoIP SR and convergence switch.
- The outer S-VLAN, which identifies services and physical locations, can be allocated based on the OLT, PON board, or PON port. The inner C-VLAN identifies services or users.

VLAN Planning and VLAN Translation Policy on Ethernet Cascading Networks

Application Scenario	VLAN Plan	VLAN Translation	
		MDU/GE Remote Extended Subrack	OLT/Master Subrack
FTTB or FTTC Ethernet cascading (MDUs serving as independent nodes)	One-tag VLAN solution	Without HGWs and with voice services provided by the MDU: Each MDU uses the same S-VLAN for its voice users. LAN access with voice services provided by HGWs: MDUs translate user VLANs to C-VLANs. xDSL access with voice services provided by HGWs: ● ATM upstream transmission: MDUs translate PVCs to C-VLANs (PVC <-> C-VLAN). ● PTM upstream transmission: Untagged upstream packets of HGWs: MDUs map C-VLANs based on user ports. User-VLAN-tagged upstream packets of HGWs: MDUs translate user VLANs to C-VLANs (user VLAN <-> C-VLAN).	The OLT transmits packets transparently.

Copyright © Huawei Technologies Co., Ltd.

Application Scenario	VLAN Plan	VLAN Translation	
		MDU/GE Remote Extended Subrack	OLT/Master Subrack
FTTB or FTTC Ethernet cascading (centralized management for GE remote extended subracks)		xDSL access with voice services provided by HGWs: ● ATM upstream transmission: The extended subrack translates PVCs to C-VLANs (PVC <-> C-VLAN). ● PTM upstream transmission: Untagged upstream packets of HGWs: The extended subrack maps C-VLANs based on user ports. User-VLAN-tagged upstream packets of HGWs: The extended subrack translates user VLANs to C-VLANs (user VLAN <-> C-VLAN).	The master subrack transmits packets transparently.

VoIP data plan based on H.248 or SIP

Item			Remarks
MG interface/ SIP interface data **NOTE** (Must be the same as that on the MGC or IMS core network device.)	Media and signaling parameters	Media and signaling upstream VLAN	Upstream VLANs of the VoIP service
		Media and signaling upstream port	Upstream ports of the VoIP service
		Media IP address and signaling IP address	Separating media streams from signaling streams
		Default IP address of the MG	Next hop IP address from an ONU/HGW to an MGC/IMS
	MG interface/SIP interface ID		-

Copyright © Huawei Technologies Co., Ltd.

Item		Remarks
	Signaling port ID	Choose the transmission method according to the requirement on the MGC/IMS side.
	IP address of primary MGC (H.248)/IP address of primary IMS device (SIP)	When dual homing is not configured, the parameters of the primary MGC need to be configured. When dual homing is configured, the IP address and the port ID of the secondary MGC must also be configured.
	Port ID of primary MGC (H248)/port ID of primary IMS device (SIP)	
	Codec mode	The codec mode is selected according to the requirements on the MGC/IMS side. Generally, the text mode is used.
	Transmission mode	The transmission mode is selected according to the requirements on the MGC/IMS side. Generally, UDP is used.
	Home domain name (SIP)	-
	Profile index (SIP)	-
	H.248 version used for starting negotiation	V1, V2 or V3 (default value). The interface may fail to register because some softswitches do not support V3.
VoIP user configuration data	Phone number	H.248: The phone numbers allocated by the MGC need to be determined, and the paging numbers for users' emergency standalone need to be planned if the emergency standalone function is provided. SIP: The phone number that the IMS core network device allocates to the user must be configured.
	TID (H.248)	If the TID template with which the PSTN user is bound does not support terminal layering, this parameter needs to be configured.
	User priority	According to the service requirements, user priorities must be specified. The user priorities include the following: ● cat1: government1 (category 1 government users) ● cat2: government2 (category 2 government users) ● cat3: normal (common users). This is the default value.

Copyright © Huawei Technologies Co., Ltd.

Item		Remarks
	User type	According to the service requirements, user type needs to be specified. The user type includes the following: ● DEL: direct exchange lines (default) ● ECPBX: earth calling PBX ● LCPBX: loop calling PBX ● PayPhone: pay phone
Common Parameter	System parameter	The system parameters, including the international version flag and message waiting indication (MWI) mode, need to be configured according to local standards to ensure that the response of the user terminal complies with the local standards.
	International parameters	The attributes such as the upper and lower thresholds of the flash-hooking duration need to be configured according to the local standards to ensure that the response of the user terminal complies with the local standards.
	PSTN port attributes	If the PSTN port needs to support the polarity reversal accounting, the PSTN port needs to be configured to support the polarity reversal pulse. Other attributes do not need to be modified if there is no special requirement.
	Ringing current attributes	When the attributes of ring current are changed, ring volume is changed. This parameter needs to be modified according to the local standard only when the default ring current attribute does not comply with the local standard.

11.2.6 Principle of IPTV Service Data Plan

The IPTV service plan mainly includes the plan of VLANs and VLAN translation policies in different network scenarios, and the plan of IPTV services.

IPTV services include multicast service and VoD service. These two services have relationships and independence in VLAN planning.

Copyright © Huawei Technologies Co., Ltd.

VLAN and VLAN translation policy

Application Scenario	Service Type	VLAN Plan	VLAN Translation		Remarks
			ONU	OLT	
Scenario 1: FTTB +HGW networking (ONU providing the VoIP service) and Scenario 2: FTTB +HGW networking (HGW providing the VoIP service)	Multicast service	One-tagged VLAN	1. The multicast VLAN (MVLAN) of the HGW is different from the network-side MVLAN. ● Upstream IGMP: The ONU performs IGMP proxy to terminate IGMP packets transmitted from the user side and encapsulate IGMP packets transmitted by network-side MVLANs. ● Downstream multicast service flows: The ONU replicates multicast packets based on user ports and multicasts downstream multicast packets across VLANs: user VLAN <-> MVLAN	● Upstream IGMP: The OLT performs IGMP proxy to terminate IGMP packets transmitted from the user side and encapsulate IGMP packets transmitted by network-side MVLANs. ● The OLT replicates multicast packets based on PON ports with MVLANs unchanged.	This solution is recommended because carriers will define a unified MVLAN on the HGW.

Copyright © Huawei Technologies Co., Ltd.

Application Scenario	Service Type	VLAN Plan	VLAN Translation		Remarks
			ONU	OLT	
	Multicast VoD service	One-tagged VLAN	VLAN translation policy: ● When packets sent from the HGW using LAN upstream transmission carries user VLANs, the ONU translates user VLANs to C-VLANs. ● When packets are sent from the HGW using xDSL upstream transmission, the ONU translates PVCs to C-VLANs.	Transparently transmits packets.	This solution is recommended. The PSPV mode is recommended for the VoD service because the service requires fewer VLANs.

Copyright © Huawei Technologies Co., Ltd.

Application Scenario	Service Type	VLAN Plan	VLAN Translation		Remarks
			ONU	OLT	
FTTB or FTTC Ethernet cascading (MDUs serving as independent nodes)	Multicast service	One-tag VLAN solution	● Upstream IGMP packets: The MDU performs IGMP proxy to terminate IGMP packets transmitted from the user side, encapsulate the packets with an MVLAN tag on the network side, and send the packets upstream. ● Downstream multicast service flows: The MDU replicates multicast packets based on user ports and multicasts downstream packets among MVLANs.	● Upstream IGMP packets: The OLT performs IGMP proxy to terminate IGMP packets transmitted from the user side, encapsulate the packets with an MVLAN tag on the network side, and send the packets upstream. ● Downstream multicast service flows: The OLT replicates multicast packets based on GE ports with MVLANs unchanged.	This solution is recommended.

Copyright © Huawei Technologies Co., Ltd.

Application Scenario	Service Type	VLAN Plan	VLAN Translation		Remarks
			ONU	OLT	
	Multicast VoD service	One-tag VLAN solution	HGWs (LAN upstream transmission): MDUs translate user VLANs to C-VLANs (user VLAN <-> C-VLAN). HGWs (xDSL upstream transmission): ● ATM upstream transmission: MDUs translate PVCs to C-VLANs (PVC <-> C-VLAN). ● PTM upstream transmission: Untagged upstream packets of HGWs: MDUs map C-VLANs based on user ports. User-VLAN-tagged upstream packets of HGWs: MDUs translate user VLANs to C-VLANs (user VLAN <-> C-VLAN).	The OLT transmits packets transparently.	This solution is recommended.

Copyright © Huawei Technologies Co., Ltd.

Application Scenario	Service Type	VLAN Plan	VLAN Translation		Remarks
			ONU	OLT	
FTTB or FTTC Ethernet cascading (centralized management for GE remote extended subracks)	Multicast service	One-tag VLAN solution	HGWs (xDSL upstream transmission) when MVLANs on HGW side and network side are different: ● Upstream IGMP packets: The extended subrack performs IGMP proxy to terminate IGMP packets transmitted from the user side, encapsulate the packets with an MVLAN tag on the network side, and send the packets to the extending board. ● Downstream multicast service flows: The extended subrack replicates multicast packets based on user ports, and multicasts the packets among MVLANs (user VLAN <- MVLAN).	● Upstream IGMP packets: The master subrack performs IGMP proxy to terminate IGMP packets transparently transmitted from the extending board and reported by the extended subrack, encapsulate the packets with an MVLAN tag on the network side, and send the packets to the upper-layer network. ● Downstream multicast service flows: The control board in the master subrack replicates multicast packets based on Ethernet extending boards, and the Ethernet extending boards replicate multicast	This solution is recommended.

Copyright © Huawei Technologies Co., Ltd.

Application Scenario	Service Type	VLAN Plan	VLAN Translation		Remarks
			ONU	OLT	
				packets based on GE ports with MVLANs unchanged.	
	Multicast VoD service	One-tag VLAN solution	HGWs (xDSL upstream transmission): ● ATM upstream transmission: The extended subrack translates PVCs to C-VLANs (PVC <-> C-VLAN). ● PTM upstream transmission: Untagged upstream packets of HGWs: The extended subrack maps C-VLANs based on user ports. User-VLAN-tagged upstream packets of HGWs: The extended subrack translates user VLANs to C-VLANs (user VLAN <-> C-VLAN).	The master subrack transmits packets transparently.	This solution is recommended.

Note

Copyright © Huawei Technologies Co., Ltd.

- IPTV service is a closed service self-operated by carriers, and one-tagged S-VLAN is recommended.
- The same S-VLAN or different S-VLANs can be used as the MVLAN and VoD VLAN. It is recommended that you use different S-VLANs as MVLAN and VoD VLAN so that the upper-layer device can easily differentiate the BTV service and VoD service.
- S-VLANs of VoD service can identify services and physical locations based on an entire network or an OLT. It is recommended that you set different VoD VLANs for the OLTs connected to one IPTV SR to avoid an excessively large broadcast domain of the SR and convergence switch.

Data plan for multicast service

Data Item	Remarks
Multicast protocol	The OLT and ONU generally use IGMP proxy. The ONT or HGW generally uses IGMP snooping.
IGMP version	The compatibility policies of the IGMP version on access equipment distinguish between the network side and the user side. 1. In normal application scenarios, the device is usually the active initiating party. The IGMP version on the multicast router can be seamlessly degraded without packet loss. 2. The terminals are always the active initiating party and can be seamlessly degraded without packet loss. The recommended versions are as follows: ● If the network-side version is V2, the recommended version for the access equipment is V2. ● If the network-side version is V3, the recommended version for the access equipment is V2 or V3. ● If the user-side version is V2, the recommended version for the access equipment is V2 or V3. ● If the user-side version is V3, the recommended version for the access equipment is V3.
Multicast program	Static configuration is recommended. The OLT can also generate a multicast program library. In other words, the OLT dynamically generates a program list according to the programs requested by users. In this mode, the program list does not need to be configured or maintained; however, the functions such as program management, user multicast bandwidth management, program preview, and program prejoin are not supported.
Multicast preview profile	Default
Multicast fast leave	Enabling this function is recommended. It reduced the exchange of IGMP packets, saving the bandwidth resources.

Copyright © Huawei Technologies Co., Ltd.

11.2.7 Principle of Security Data Plan

The security plan involves system security plan, user security plan, and service security plan. Security policy ensures service security from different aspects.

NOTE

- The device provides complete security measures, but not all security measures need to be deployed. Only the security measures that meet the following requirements need to be deployed:
  - The security measures can be used on the live network.
  - The security measures are easy to deploy.
  - The security measures are effective.
- Different ONUs support different security features. Select the security feature recommended in this topic according to actual ONU capabilities.

System Security

Security Vulnerability	Solution	Description and Usage Suggestion
DoS attack	Enable the anti-DoS-attack function for OLT and MDU.	After the anti-DoS-attack function is enabled, control packets are monitored and those exceeding the number threshold are discarded. Use this solution for new site deployment.
IP attack	Enable the anti-IP-attack function for OLT and MDU.	After the anti-IP-attack function is enabled, a device discards the IP packets received from the user side whose destination IP address is the IP address of the device, and therefore the system is protected. Use this solution for new site deployment.

Copyright © Huawei Technologies Co., Ltd.

User Security

Security Vulnerability	Solution	Description and Usage Suggestion
MAC spoofing	Enable the anti-MAC-duplicate function for OLT and MDU.	After anti-MAC-duplicate is enabled, the system records the first MAC address learnt from the port and binds the MAC address to the port and VLAN. If receiving packets sent from the host that has the same MAC address with the port, the system discards the packets directly. In this case, it can prevent users from forging MAC addresses to perform malicious attacks. Use this solution for new site deployment.
MAC attack	Enable the anti-MAC spoofing function for OLT and MDU.	After anti-MAC spoofing is enabled, the system can prevent users from forging IP addresses to perform malicious attacks. Use this solution for new site deployment.
IP spoofing	Enable the anti-IP spoofing function for MDU.	After anti-IP spoofing is enabled, the system can prevent users from forging IP addresses to perform malicious attacks. Use this solution for new site deployment.

Copyright © Huawei Technologies Co., Ltd.

Service Security

Security Vulnerability	Solution	Description and Usage Suggestion
Unauthorized broadband access of small enterprises (IPoE)	DHCP option 82 is enabled on OLT and MDU, and the BRAS implements user authentication based on the RAIO information.	In the DHCP option 82 mode, user's physical location is added to the option 82 field carried in the DHCP request packet initiated by a user. The physical location, used for user authentication on the upper-layer authentication server, can help implement the following functions: ● The DHCP relay forwards DHCP response packets to devices with specified CID and RID. ● Prevents DHCP address exhaustion. ● Achieves static allocation of DHCP addresses. ● Implements anti-IP spoofing. ● Implements anti-user ID spoofing. ● Implements anti-MAC spoofing. Use this solution for the DHCP Internet access service.
Broadband access of residential users (PPPoE), user account theft/ borrowing	PPPoE+ (PITP) is enabled on OLT and MDU, and the BRAS implements user authentication based on binding of the RAIO information to the user account.	The BRAS responds to request packets of users with specified CID and RID. In this way, the following functions are implemented: ● Prevents IP address exhaustion. ● Implements anti-IP spoofing. ● Implements anti-user ID spoofing. ● Implements anti-MAC spoofing. Use this solution for the PPPoE Internet access service.

11.3 Configuring Services in Various FTTB and FTTC Scenarios (GPON and 10G GPON Access)

This topic describes how to configure the Internet access service, voice service and multicast service in GPON/10G GPON access mode in FTTB/FTTC networking scenarios.

Copyright © Huawei Technologies Co., Ltd.

Context

There are two xPON configuration modes: distributed mode (also called discrete mode) and profile mode. The difference between the two modes lies in command lines.

- Distributed mode: In this mode, ONTs need to be configured one by one but not in batches.
- Profile mode: In this mode, an ONT line profile and service profile are configured first. Then, ONTs can be added in batches by binding profiles. This mode greatly improves service provisioning efficiency.

Generally, the xPON configuration mode is determined in a new deployment and will not be changed.

NOTE

For commands for the distributed configuration mode, see **PON distributed-mode commands** in the *Command Reference*.

The description of this topic is based on the mode below. You can query the current mode in the diagnosis mode.

Mode	Query Method
GPON profile mode (system default)	huawei(config)#**diagnose** huawei(diagnose)%%**display xpon mode** ---------- Current config mode: Profile-mode ----------
ADSL2+ common mode (RFC2662 mode)	huawei(config)#**diagnose** huawei(diagnose)%%**display xdsl mode** ---------- ADSL Current mode : rfc2662 VDSL Current mode : tr129 ----------
VDSL2 common mode (TR129 mode)	

11.3.1 FTTB Networking (LAN Access Without HGW)

In FTTB networking (LAN access without the HGW), the ONU provides 100M FE access and POTS access for Internet access service and VoIP service respectively for users. This topic describes how to configure the Internet access service and VoIP service on the OLT and ONU in FTTB networking.

11.3.1.1 Service Requirements and Application Scenarios

FTTB networking is usually used in trade estate and housing estate having high-density buildings and users. In FTTB networking, optical fibers are connected from the central office (CO) to buildings. The network section from the service convergence nodes to users is deployed by xDSL or LAN access. LAN access is easily and commonly deployed and therefore becomes the first choice for bandwidth construction.

Service Requirements

Only Internet access service and VoIP service are supported and there is no multicast requirement.

Copyright © Huawei Technologies Co., Ltd.

Considering simple and flexible service provisioning and easy OM, category-5 cables and FTTB (LAN access) are used for deployment.

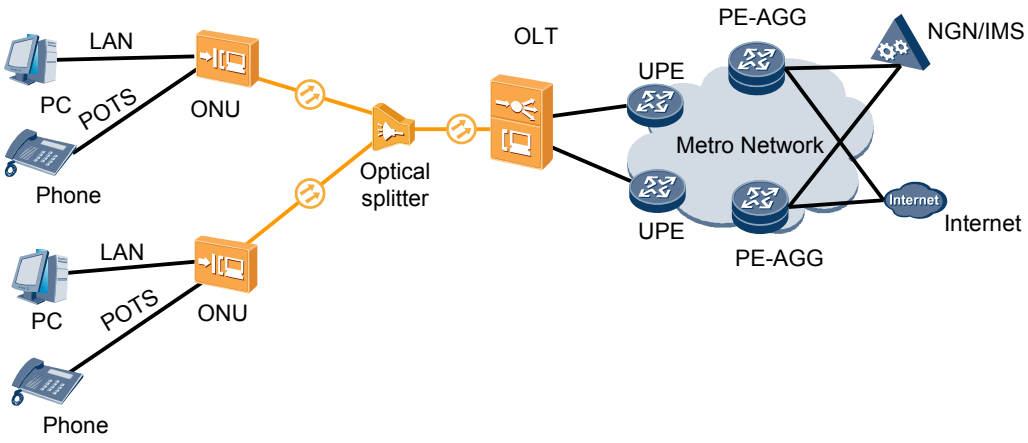
Application Scenarios

As shown in **Figure 11-3**, the ONU is deployed in the building and is connected to the user's home through the category-5 cable.

- For the Internet access service: Users are connected to the ONU through category-5 cables and are authenticated by dialup using PCs. Each user has an independent account and is authenticated and managed on the BRAS.
- For the VoIP service: Users are provisioned with the VoIP service through the ONU with the build-in voice module.

ONU for FTTB networking: MA5616, MA5822, MA5612.

Figure 11-3 Example network of the FTTB service (LAN access)

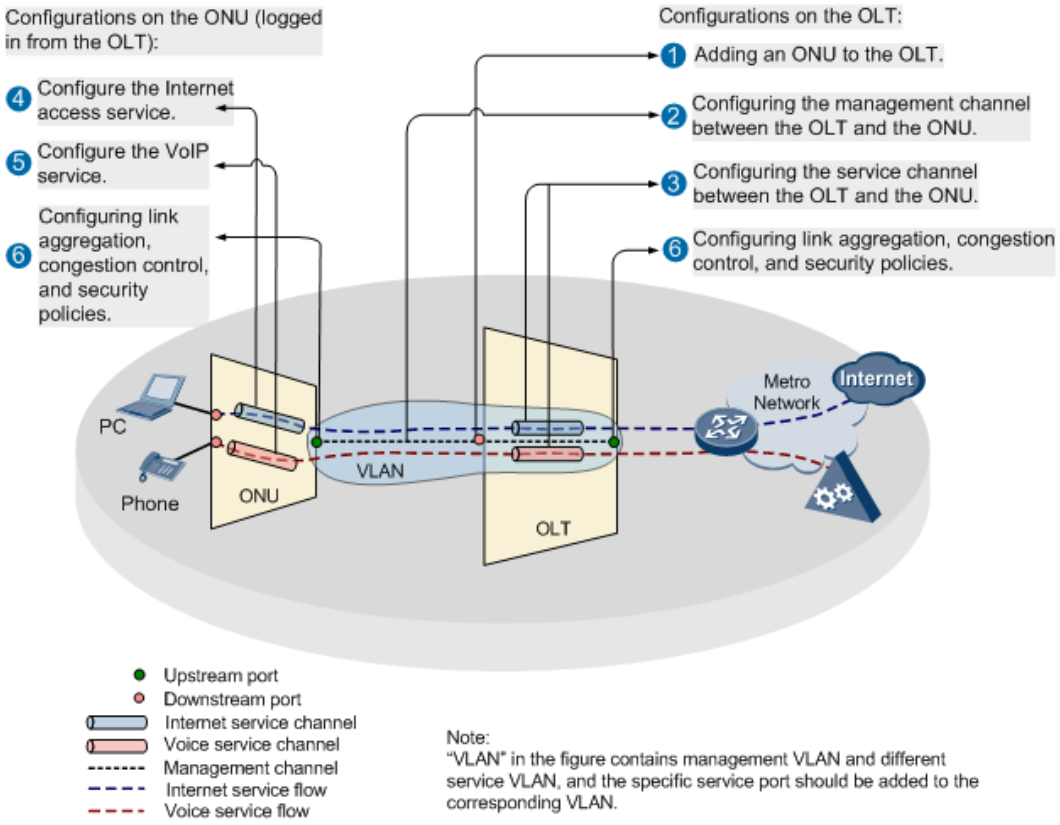


11.3.1.2 Configuration Procedure

Figure 11-4 shows the configuration roadmap diagram in the FTTB and FTTC networking scenarios using LAN access without HGWs.

Copyright © Huawei Technologies Co., Ltd.

Figure 11-4 Configuration Roadmap Diagram in the FTTB and FTTC Networking Scenarios Using LAN Access Without HGWs



The following table lists the detailed description steps..

Item	Procedure		Remarks
OLT	**Add an ONU to the OLT.**		Services can be configured for an ONU only after the ONU is successfully added to an OLT.
	Configure the management channel between the OLT and the ONU.		After the inband management channel between the OLT and the ONU is configured and available, you can log in to the ONU from the OLT to configure the ONU.
	Configure the service channel between the OLT and the ONU.	● Configure the Internet access service channel. ● Configure the VoIP service channel.	The ONU provides only the Internet access service and the VoIP service in the FTTB and FTTC network using xDSL access without HGWs. Therefore, you need to create an Internet access service channel and a VoIP service channel on the OLT.

Copyright © Huawei Technologies Co., Ltd.

Item	Procedure		Remarks
ONU	**Configure the Internet access service.**		This topic describes how to configure the Internet access service through the Ethernet port by the ONU. Specifically, configure service flows on the ONU and configure the upstream VLAN to provide the service channel from the ONU to the user and set up the upstream channel from the ONU to the OLT.
	Configure the VoIP service	**Configure the H.248 VoIP service on the ONU.**	**NOTE** The H.248 and SIP protocols are mutually exclusive for the VoIP service. Only one of them is configured at a time.
		Configure the SIP VoIP service on the ONU.	
OLT ONU	**Configure the link aggregation, congestion control, and security policy.**		The global configuration of upstream link aggregation and queue scheduling based on priorities ensures service reliability. The global configuration of security policies ensures service security.
ONU	**Verify the service.**		The ONU provides remote verification methods including PPPoE dialup emulation and call emulation for configuration and commissioning engineers to verify services remotely after service configuration, avoiding a second on-site operation.

11.3.1.3 Adding an ONU to an OLT

Services can be configured for an ONU only after the ONU is successfully added to an OLT.

Context

- When an ONU is added, corresponding profiles need to be bound to the ONU, including the dynamic bandwidth allocation (DBA) profile, line profile, and alarm profile. For details about functions and configuration methods for these profiles, see **Table 11-5**.

Copyright © Huawei Technologies Co., Ltd.

Table 11-5 Introduction to ONU profiles

Profile Type	Function	Command
DBA profile	A DBA profile describes GPON traffic parameters. A T-CONT is bound to a DBA profile for dynamic bandwidth allocation, improving upstream bandwidth utilization.	Query a DBA profile. **display dba-profile** Add a DBA profile. **dba-profile add**
Line profile	A line profile describes binding between the T-CONT and the DBA profile, the QoS mode of the service flow, and mapping between the GEM port and the ONU-side service.	Query a line profile. **display ont-lineprofile** Add a line profile. **ont-lineprofile add**
Alarm profile	An alarm profile contains a series of alarm threshold parameters that are used for performance measurement and monitoring of the activated ONT lines.	Query an alarm profile. **display gpon alarm-profile** Add an alarm profile. **gpon alarm-profile add**

- An ONU can be added in two modes. Select either mode as required.

Mode	Usage Scenario	Command
Add an ONU offline.	The ONU password or serial number (SN) is obtained.	Run the **ont add** command to add an ONU.
Online confirm an ONU.	Both the ONU password and SN are not obtained.	In the GPON mode, run the **port ont-auto-find** command to enable the ONU auto-discovery function of a GPON port and then run the **ont confirm** command to add an ONU.

Data plan

Table 11-6 Data plan

Item	Data
DBA profile	Profile name: fttb_dba Profile type: type3 Assured bandwidth: 8 Mbit/s Maximum bandwidth: 20 Mbit/s

Copyright © Huawei Technologies Co., Ltd.

Item	Data
Line profile	Profile name: fttb(c) Profile ID: 10 T-CONT ID: 4 GEM port ID for management service: 11 GEM port ID for Internet access service: 12 GEM port ID for VoIP service: 13
Network topology data	PON port: 0/2/1 ONT ID: 1

Procedure

Step 1 Configure GPON ONU profiles.

1. Configure a DBA profile.

   ```
   huawei(config)#dba-profile add profile-name fttb_dba type3 assure 8192 max 20480
   ```

2. Configure an ONU line profile.

   a. Add GPON ONU line profile 10 fttb(c).

   ```
   huawei(config)#ont-lineprofile gpon profile-id 10 profile-name fttb(c)
   ```

   NOTE

   The ID of the line profile to be created must not exist in the system and the line profile must be created according to the data plan. In this example, line profile 10 is used.

   b. In the line profile mode, bind T-CONT 4 to DBA profile fttb_dba.

   ```
   huawei(config-gpon-lineprofile-10)#tcont 4 dba-profile-name fttb_dba
   ```

   c. In the line profile mode, bind the GEM port to the T-CONT.

   - Add GEM port 11 to carry management service flows.
   - Add GEM port 12 to carry Internet access service flows.
   - Add GEM port 13 to carry VoIP service flows.

   Bind GEM ports 11, 12, and 13 to T-CONT 4. In configuring, QoS policies for various service flows also need to be configured. For details about QoS data plan, see **11.2.2 Principle of QoS Data Plan**.

   ```
   huawei(config-gpon-lineprofile-10)#gem add 11 eth tcont 4 cascade on
   huawei(config-gpon-lineprofile-10)#gem add 12 eth tcont 4 cascade on
   huawei(config-gpon-lineprofile-10)#gem add 13 eth tcont 4 cascade on
   ```

   d. Configure mapping between the GEM port and the ONU-side service.

   Set the mode for mapping the GEM port to the ONU-side service to the VLAN mapping mode (default). Map management service flows (the CVLAN ID is 8) to GEM port 11, Internet access service flows (the CVLAN ID is 1001) to GEM port 12, and VoIP service flows (the CVLAN ID is 200) to GEM port 13.

   ```
   huawei(config-gpon-lineprofile-10)#gem mapping 11 0 vlan 8
   huawei(config-gpon-lineprofile-10)#gem mapping 12 1 vlan 1001
   huawei(config-gpon-lineprofile-10)#gem mapping 13 2 vlan 200
   ```


Copyright © Huawei Technologies Co., Ltd.

e. After the configuration is completed, run the **commit** command to make the configured parameters take effect.

```
huawei(config-gpon-lineprofile-10)#commit
huawei(config-gpon-lineprofile-10)#quit
```

3. (Optional) Add an alarm profile.
   - The ID of the default GPON alarm profile is 1. The thresholds for all the alarm parameters in the default alarm profile are 0, which indicates that no alarm is generated.
   - In this example, the default alarm profile is used and therefore the configuration of the alarm profile is not required.

Step 2 Add an ONU to an OLT.

Assume that the ID of GPON port 0/2/1 is 1, SN is 32303131B39FD641, management mode is SNMP, and the bound line profile is fttb(c). Connect the ONU to such a GPON port through the optical splitter.

There are two modes to add an ONT: add an ONT offline and confirm an automatically discovered ONU.

- Add an ONU offline.

```
huawei(config)#interface gpon 0/2
huawei(config-if-gpon-0/2)#ont add 1 ontid 1 sn-auth 32303131B39FD641
snmp ont-lineprofile-name fttb(c)
```

- Confirm an automatically discovered ONU.

```
huawei(config)#interface gpon 0/2
huawei(config-if-gpon-0/2)#port 1 ont-auto-find enable
huawei(config-if-gpon-0/2)#display ont autofind 1
huawei(config-if-gpon-0/2)#ont confirm 1 ontid 1 sn-auth 32303131B39FD641
snmp ont-lineprofile-name fttb(c)
```

1. (Optional) Bind the alarm profile to the ONU.

   By default, alarm profile 1 automatically bound to an ONU. A non-default alarm profile is bound manually only when the default one does not meet the requirement.

   In this example, default alarm profile 1 is used and therefore the configuration of the alarm profile is not required.

Step 3 Check the ONU status.

After an ONU is added, run the **display ont info** command to query the current status of the ONU. Ensure that **Config flag** of the ONU is **active**, **Run State** is **online**, and **Config state** is **normal**.

```
huawei(config-if-gpon-0/2)#display ont info 1 1
  ------------------------------------------------------------------------
  F/S/P                : 0/2/1
  ONT-ID               : 1
  Control flag         : active    //The ONU is activated.
  Run state            : online    //The ONU is online.
  Config state         : normal    //The ONU configurations are recovered
normally.
...//The rest of the response information is not provided here.
huawei(config-if-gpon-0/2)#quit
```

----End

Follow-up Procedure

When **Config state** is **failed**, **Run state** is **offline**, or **Match state** is **mismatch**:

Copyright © Huawei Technologies Co., Ltd.

- If **Control flag** is **deactive**, run the **ont active** command in GPON mode to activate the ONU.
- If **Run state** is **offline**, a physical line may be broken or the optical module may be damaged. Check the line and the optical module.
- If **Config state** is **failed**, the configured ONU capability exceeds the actual ONU capability. In this case, run the **display ont failed-configuration** command in the diagnose mode to check the failed configuration item and the failure cause. Then, rectify the fault accordingly.
- If the ONU does not match, that is, **Match state** is **mismatch**, the port types and number of ports undermatch the actual port types and number of ports supported by the ONU. In this case, run the **display ont capability** command to query the actual capability of the ONU, and then select one of the following modes to modify the ONU configuration:
  - Create a proper ONU profile according to the actual capability of the ONU, and then run the **ont modify** command to modify the configuration data of the ONU.
  - Modify the ONU profile according to the actual capability of the ONU and save the modification. Then, the ONU automatically recovers the configuration successfully.

11.3.1.4 Configuring the Management Channel Between the OLT and the ONU

After the inband management channel between the OLT and the ONU is configured and available, you can log in to the ONU from the OLT to configure the ONU.

Data plan

Item	Data	Remarks
Management VLAN and management IP address on the OLT side	Management VLAN ID: 8 Management VLAN type: smart VLAN Inband management IP address: 192.168.50.1/24	To configure the MDU from the OLT by remote logging in to the MDU, the management VLAN of the OLT and that of the MDU must be the same, and the management IP address of the OLT and that of the MDU must be in the same network segment.
Management VLAN and management IP address on the ONU side	Management VLAN ID: 8 Management VLAN type: smart VLAN Inband management IP address: 192.168.50.2/24	

Procedure

Step 1 Configure the inband management VLAN and IP address of the OLT.

Configure the inband management VLAN to 8, VLAN priority to 6, and the IP address to 192.168.50.1/24.

```
huawei(config)#vlan 8 smart
huawei(config)#port vlan 8 0/19 0
huawei(config)#vlan priority 8 6
huawei(config)#interface vlanif 8
```


Copyright © Huawei Technologies Co., Ltd.

```
huawei(config-if-vlanif8)#ip address 192.168.50.1 24
huawei(config-if-vlanif8)#quit
```

Step 2 Configure the inband management VLAN and IP address of the ONU.

Configure the static IP address of the ONU to 192.168.50.2/24, gateway to 192.168.50.254, and the management VLAN ID to 8 (the same as the management VLAN of the OLT).

```
huawei(config)#interface gpon 0/2
huawei(config-if-gpon-0/2)#ont ipconfig 1 1 static ip-address 192.168.50.2 mask
255.255.255.0 gateway
192.168.50.254 vlan 8
huawei(config-if-gpon-0/2)#quit
```

Step 3 Configure an inband management service port.

Configure the management service port ID to 1, management VLAN ID to 8, GEM port ID to 11, and user-side VLAN ID to 8. The OLT does not limit inband management service flows. Therefore, it is recommended that you use default traffic profile 6.

```
huawei(config)#service-port 1 vlan 8 gpon 0/2/1 ont 1 gemport 11 multi-service
user-vlan 8 rx-cttr 6 tx-cttr 6
```

Step 4 Confirm that the management channel between the OLT and the ONU is available.

- On the OLT, run the **ping** ***192.168.50.2*** command to check the connectivity between the OLT and the ONU. The ICMP ECHO-REPLY packet from the ONU should be received.
- On the OLT, you can remote log in to the ONU to perform the configuration.

----End

11.3.1.5 Configuring the Service Channel Between the OLT and the ONU

Various service flows can be configured on the OLT for different services so that service packets on the ONU can be forwarded at Layer 2 according to the planned VLAN and forwarding policies.

Context

Service flows can be added in two modes, as described in **Table 11-7**. Select either mode as required.

Table 11-7 Adding service flows

Mode	Command	Remarks
Add service flows one by one.	**service-port**	-
Add service flows in batches.	**multi-service-port**	You need to specify the **ontid** + **gemindex** to identify a service flow and ensure that the number of GEM ports is the same as the number of VLANs on the user side.

Copyright © Huawei Technologies Co., Ltd.

Data plan

Item	Data	Remarks
Internet access service	OLT VLAN ID: ● CVLAN ID: 256 x GPON port ID + 32 x Split ratio x (Splitter port ID - 1) + ONU port ID + 1 ● SVLAN: VLAN ID 100 and attribute stacking Upstream VLANs of the ONU: 1001-1016 Service flow ID: 101	Assume that the split ratio of the optical splitter is 1:32, the ONU is connected to port 1 on the optical splitter using the optical cable, and the user PC is connected to port 1 on the ONU. In this case, the inner VLAN is 258 according to the formula for calculating the inner VLAN. For details about the data plan, see **11.2.3 Principle of Internet Access Service Data Plan**.
VoIP service	OLT VLAN ID (VLAN transparently transmitting the ONU service): 200 ONU VLAN ID: 200 Service flow ID: 201	For details about the data plan, see **11.2.5 Principle of VoIP Service Data Plan**.

Procedure

- Configure the channel for the Internet access service.
  1. Configure the service VLAN and add the upstream port to this VLAN.

     Configure the SVLAN ID to 100, VLAN type to smart VLAN, and VLAN attribute to stacking. Add upstream port 0/19/0 to VLAN 100.

     ```
     huawei(config)#vlan 100 smart
     huawei(config)#vlan attrib 100 stacking
     huawei(config)#port vlan 100 0/19 0
     ```

  2. Configure the corresponding traffic profile.

     The 802.1p priority for the Internet access service is 0 and the traffic profile is unlimited. You can run the **display traffic table ip** command to query the traffic profile in the system. Use traffic profile 6.

     ```
     huawei(config)#display traffic table ip from-index 0
     ```

  3. Configure service flows to receive and transparently transmits the Internet access service from the ONU.

     According to the data plan,

     - For the OLT: The SVLAN ID is 100, inner VLAN ID is 258. The user-side VLAN ID of the OLT is the same as the upstream VLAN ID of the ONU, that is, 1001. The Internet access service uses GEM port 12.
     - For the ONU: The upstream VLAN ID is 1001.

     ```
     huawei(config)#service-port 101 vlan 100 gpon 0/2/1 ont 1 gemport 12 multi-service
     ```


Copyright © Huawei Technologies Co., Ltd.

```
user-vlan 1001 tag-transform translate-and-add inner-vlan 258 rx-cttr 6 tx-
cttr 6
```

- Configure the channel for the VoIP service.
  1. Configure the service VLAN and add the upstream port to this VLAN.

     Configure the SVLAN ID to 200 and VLAN type to smart VLAN. Add upstream port 0/19/0 to VLAN 200.

     ```
     huawei(config)#vlan 200 smart
     huawei(config)#port vlan 200 0/19 0
     ```

  2. Configure the corresponding traffic profile.

     The 802.1p priority of the VoIP service is 5 and the traffic profile is unlimited. You can run the **display traffic table ip** command to query the traffic profile in the system. If the existing traffic profile does not meet data plan requirements, a new traffic profile is required.

     New traffic profile 9 is added. In the command execution, *priority-policy* is **local-setting**, which indicates that service packets are scheduled by the priority specified in the traffic profile.

     ```
     huawei(config)#traffic table ip index 9 cir off priority 5 priority-policy
     local-setting
     ```

  3. Configure service flows to receive and transparently transmits the VoIP service from the ONU.

     According to the data plan,

     - For the OLT: The SVLAN ID is 200. The user-side VLAN ID of the OLT is the same as the upstream VLAN ID of the ONU, that is, 200. The VoIP service uses GEM port 13.
     - For the ONU: The upstream VLAN ID is 200.

     ```
     huawei(config)#service-port 201 vlan 200 gpon 0/2/1 ont 1 gemport 13 multi-
     service
     user-vlan 200 rx-cttr 9 tx-cttr 9
     ```

----End

11.3.1.6 Configuring LAN Internet Access Service (On the ONU)

This topic describes how to configure the Internet access service through the Ethernet port by the ONU. Specifically, configure service flows on the ONU and configure the upstream VLAN to provide the service channel from the ONU to the user and set up the upstream channel from the ONU to the OLT.

Context

In this example, the ONU is in version V800R310C00. For ONU in other versions, configurations are slightly different. For details, see the corresponding Configuration Guide.

Copyright © Huawei Technologies Co., Ltd.

Data plan

Item	Data	Remarks
Port	Upstream port: 0/0/1 Service port: 0/3/1	-
Service VLAN	VLAN ID: 1001-1016 VLAN type: smart VLAN VLAN attribute: common	The ONU supporting 16 FE ports is used as an example. In actual configuration, plan the data according to actual capabilities of devices. For details about the data plan, see **11.2.3 Principle of Internet Access Service Data Plan**.
Traffic profile	Profile ID: 8 Committed rate: 4 Mbit/s Priority: 0	For details about the data plan, see **11.2.2 Principle of QoS Data Plan**.

Procedure

Step 1 Log in to and configure the ONU.

You can remote log in to the ONU from the OLT to perform the configuration. The user name is **root** and the password is **mduadmin**.

Step 2 Create SVLANs.

Create smart SVLANs 1001-1016 in batches with attribute common.

```
huawei(config)#vlan 1001-1016 smart
```

Step 3 Add the upstream port to SVLANs.

Add upstream port 0/0/1 to SVLANs.

```
huawei(config)#port vlan 1001-1016 0/0 1
```

Step 4 Configure a traffic profile.

Run the **display traffic table ip** command to query the existing traffic profiles in the system. If the existing traffic profile in the system does not meet the requirement, run the **traffic table ip** command to add a traffic profile.

Assume that the committed information rate (CIR) is 4 Mbit/s, priority of upstream packets is 0, and downstream packets are scheduled based on the priorities specified in the traffic profile. Configure traffic profile 8.

```
huawei(config)#traffic table ip index 8 cir 4096 priority 0 priority-policy local-Setting
```

Step 5 Add a service port.

Create service port 101, bind it to port 0/3/1, set the user-side VLAN to untagged and bind the VLAN to traffic profile 8.

Copyright © Huawei Technologies Co., Ltd.

NOTE

This example creates one service port as an example. Each service port maps a user. When configuring another service port, map the corresponding SVLAN.

```
huawei(config)#service-port 101 vlan 1001 eth 0/3/1 multi-service user-vlan untagged rx-cttr 8 tx-cttr 8
```

Step 6 Save the data.

```
huawei(config)#save
```

----End

11.3.1.7 Configuring H.248 Voice Service (on the ONU)

This topic describes how to configure the voice service on the ONU based on the H.248 protocol to provide the high quality and low cost VoIP service for users.

Prerequisites

- The media gateway controller (MGC) interface data and the PSTN user data corresponding to the media gateway (MG) interface is configured on the MGC.
- Ensure that the **Status** of the voice board on the ONU is **Normal** by running the **display board 0** command.

Precautions

1. An ONU supports both the H.248 and SIP protocols; however, these two protocols are mutually exclusive. You can run the **display protocol support** command to query the currently supported voice protocol.
2. If the voice protocol needs to be switched, you need to delete the MG interface first and run the **protocol support** command to switch the protocol. After the configuration is complete, save the configuration and restart the system to make the configured protocol take effect.

CAUTION

This operation interrupts the ongoing services carried on the currently used MG interface. Hence, exercise caution when performing this operation.

Data plan

For details about the data plan, see **11.2.5 Principle of VoIP Service Data Plan**.

Item			Data
MG interface data	Media and signaling	Media and signaling upstream VLANs	200
		Media and signaling upstream port	0/0/1

Copyright © Huawei Technologies Co., Ltd.

Item			Data
NOTE The data configuration must be the same as the data configuration on the MGC.	parameters	Media IP address and signaling IP address	10.10.10.10/24
		Default gateway IP address	10.10.10.1/24
	MG interface ID		0
	Signaling port ID		2944
	IP address of the primary MGC		200.200.200.200/24
	Port ID of the primary MGC		2944
	Coding		Text
	Transmission mode		UDP
	H248 version that MG starts to negotiate		1 (the negotiation starts from V1)
Voice user configuration data	Phone number		83110001-83110024
	Terminal identification		Terminal layering is not supported and the terminal identification ranges from 0 to 23.
	User priority		Cat2 for phone 1 Cat3 for phone 2 to phone 24 (default)
	User type		Common user (DEL user by default)
Common parameter	System parameter		Default value
	Overseas parameter		Default value
	PSTN port attribute		Polarity-reversal
	Ringing current attribute		Default value

Procedure

Step 1 Log in to and configure the ONU.

You can remote log in to the ONU from the OLT to perform the configuration. The user name is **root** and the password is **mduadmin**.

Step 2 Configure the upstream VLAN interface.

Specify the upstream VLAN interface for the media stream and the signaling flows and configure the IP addresses of the Layer 3 interface. These IP addresses are the sources of the IP address pools for the media stream and the signaling flows.

Copyright © Huawei Technologies Co., Ltd.

1. Create an upstream VLAN.

   The VLAN ID is 200 and the VLAN is a smart VLAN.

   ```
   huawei(config)#vlan 200 smart
   ```

2. Add the upstream port to the created upstream VLAN.

   Add upstream port 0/0/1 to VLAN 2000.

   ```
   huawei(config)#port vlan 200 0/0 1
   ```

3. Configure the IP address of the Layer 3 interface.

   Enter the VLAN interface mode and configure the lP address of the Layer 3 interface to 10.10.10.10

   ```
   huawei(config)#interface vlanif 200
   huawei(config-if-vlanif200)#ip address 10.10.10.10 24
   huawei(config-if-vlanif200)#quit
   ```

Step 3 Configure the media and signaling IP address pools.

Configure both the media IP address and signaling IP address to 10.10.10.10 and the MG IP address to 10.10.10.1.

```
huawei(config)#voip
huawei(config-voip)#ip address media 10.10.10.10 10.10.10.1
huawei(config-voip)#ip address signaling 10.10.10.10
huawei(config-voip)#quit
```

NOTE

- You can configure the attributes of the MG interface only when the media IP address and the signaling IP address exist in the media and signaling IP address pools.
- The media IP address can be different from the signaling IP address. Plan the data according to actual networking.

Step 4 Configure static routes.

Because the IP address of the VLAN interface and the IP address (200.200.200.200/24) of the MGC are in different network segments, you need to configure a route for the network segment from gateway 10.10.10.1 to 200.200.200.0.

```
huawei(config)#ip route-static 200.200.200.0 24 10.10.10.1
```

Step 5 Add an MG interface.

Add an MG interface to communicate with the MGC, which ensures that the MGC can control the call connection through the MG interface. Add MG interface 0 according to the data plan.

```
huawei(config)#interface h248 0
  Are you sure to add MG interface?(y/n)[n]:y
```

Step 6 Configure the attributes of the MG interface.

Pay attention to the following when configuring the attributes of the MG interface according to the data plan:

- The MG interface is registered by the IP address (default mode) or domain name, which must be the same as that on the MGC.
- The negotiated H.248 protocol version is V1, V2 or V3 (default value). The interface may fail to be registered because some softswitches do not support V3.

```
huawei(config-if-h248-0)#if-h248 attribute mgip 10.10.10.10 mgport
 2944 code text transfer udp primary-mgc-ip1 200.200.200.200 primary-mgc-port
 2944 mg-media-ip1 10.10.10.10 start-negotiate-version 1
```

Step 7 Reset the MG interface.

Copyright © Huawei Technologies Co., Ltd.

```
huawei(config-if-h248-0)#reset coldstart
  Are you sure to reset MG interface?(y/n)[n]:y
huawei(config-if-h248-0)#quit
```

NOTE

- You must cold reset the MG interface after configuring. Otherwise, the MG interface does not take effect.
- The MG interface can be cold reset only after parameters mgip, mgport, primary-mgc-ip1 (or mgc-domain-name1), mgcport_1, code, transfer, and mg-media-ip are correctly configured.

Step 8 Configure the PSTN user data.

Configure phone numbers of users 0/3/0-0/3/23 to 83110001-83110024 in batches and terminal identification to 0.

- Phone numbers are used for only internal emergency standalone, that is, internal extensions call each other. Actual phone numbers are assigned by the MGC.
- If the user of the MG interface is configured to support terminal layering, you need not configure the terminal identification because the system automatically allocates it. If the user of the MG interface does not support terminal layering, the terminal identification is mandatory. The terminal identification must be unique on one MG interface.

```
huawei(config)#esl user
huawei(config-esl-user)#mgpstnuser batadd 0/3/0 0/3/23 0 terminalid 0 telno
83110001
```

Step 9 Configure the call priority of a PSTN user.

```
huawei(config-esl-user)#mgpstnuser modify 0/3/0 priority cat2
huawei(config-esl-user)#quit
```

Step 10 Configure all the PSTN ports to support polarity reversal.

Configure the physical attributes of the PSTN port to which the users belong to support polarity reversal so that the user supports polarity reversal accounting.

```
huawei(config)#pstnport
huawei(config-pstnport)#pstnport attribute batset 0/3/0 0/3/23 reverse-pole-pulse
enable
huawei(config-pstnport)#quit
```

Step 11 Save the data.

```
huawei(config)#save
```

----End

11.3.1.8 Configuring SIP Voice Service (on the ONU)

This topic describes how to configure voice services based on the Session Initiation Protocol (SIP) on an optical network unit (ONU). The voice over IP (VoIP) services have high quality, but require low cost.

Prerequisites

- The IP Multimedia Subsystem (IMS) interface data and public switched telephone network (PSTN) user data corresponding to the SIP interface is configured on the IMS.
- **Status** of the voice board on the ONU is normal. (To verify board status, run the **display board 0** command.)

Copyright © Huawei Technologies Co., Ltd.

Precautions

1. An ONU supports both the H.248 and SIP protocols; however, these two protocols are mutually exclusive. You can run the **display protocol support** command to query the currently supported voice protocol.
2. If the voice protocol needs to be switched, you need to delete the MG interface first and run the **protocol support** command to switch the protocol. After the configuration is complete, save the configuration and restart the system to make the configured protocol take effect.

CAUTION

This operation interrupts the ongoing services carried on the currently used MG interface. Hence, exercise caution when performing this operation.

Data Plan

For configuration rules and description of configuration items, see **11.2.5 Principle of VoIP Service Data Plan**.

Item			Data
SIP interface data **NOTE** (It must be the same as that on the IMS core network device.)	Media and signaling parameters	Media and signaling upstream VLAN	200
		Media and signaling upstream port	0/0/1
		Media IP address and signaling IP address	10.10.10.10/24
		Default gateway IP address	10.10.10.1/24
	SIP interface ID		0
	Signaling port ID		5060
	IP address of the main IMS equipment		200.200.200.200/24
	Port ID of the main IMS equipment		5060
	Coding scheme		Text
	Transmission mode		UDP
	Home domain name (SIP)		huawei

Copyright © Huawei Technologies Co., Ltd.

Item		Data
	Profile index (SIP)	1
Voice user configuration data	Phone number	83110001-83110024
	User priority	Phone 1 indicates Cat2. Phone 2 to phone 24 indicate Cat3 (default value).
	User type	Common user (the DEL user by default)
Common Parameter	System parameter	Default value
	Overseas parameter	Default value
	PSTN port attribute	Polarity-Reversing Pulse
	Ringing current attribute	Default value

Procedure

Step 1 Log in to and configure the ONU.

You can remote log in to the ONU from the OLT to perform the configuration. The user name is **root** and the password is **mduadmin**.

Step 2 Configure the upstream VLAN interface.

Specify the upstream VLAN interface for the media stream and the signaling flows and configure the IP addresses of the Layer 3 interface. These IP addresses are the sources of the IP address pools for the media stream and the signaling flows.

1. Create an upstream VLAN.

   The VLAN ID is 200 and the VLAN is a smart VLAN.

   ```
   huawei(config)#vlan 200 smart
   ```

2. Add the upstream port to the created upstream VLAN.

   Add upstream port 0/0/1 to VLAN 2000.

   ```
   huawei(config)#port vlan 200 0/0 1
   ```

3. Configure the IP address of the Layer 3 interface.

   Enter the VLAN interface mode and configure the lP address of the Layer 3 interface to 10.10.10.10

   ```
   huawei(config)#interface vlanif 200
   huawei(config-if-vlanif200)#ip address 10.10.10.10 24
   huawei(config-if-vlanif200)#quit
   ```

Step 3 Configure the media and signaling IP address pools.

Set the media IP address and signaling IP address to 10.10.10.10, and the media gateway to 10.10.10.1.

```
huawei(config)#voip
huawei(config-voip)#ip address media 10.10.10.10 10.10.10.1
huawei(config-voip)#ip address signaling 10.10.10.10
huawei(config-voip)#quit
```


Copyright © Huawei Technologies Co., Ltd.

NOTE

- Attributes of the MG interface can be configured only when the media IP address and the signaling IP address exist in the media and signaling IP address pools.
- The Media IP address and signaling IP address can be different. Data planning should be based on networking requirements.

Step 4 Configure static routes.

Because the IP address of the VLAN interface and that of the IMS (200.200.200.200/24) are in different network segments, the configured routes must be from gateway 10.10.10.1 to the network segment 200.200.200.0.

```
huawei(config)#ip route-static 200.200.200.0 24 10.10.10.1
```

Step 5 Add an SIP interface.

The SIP interface is used for IMS communication.

```
huawei(config)#interface sip 0
  Are you sure to add the SIP interface?(y/n)[n]:y
```

Step 6 Configure the basic attributes of the SIP interface.

```
huawei(config-if-sip-0)#if-sip attribute basic media-ip 10.10.10.10 signal-ip
 10.10.10.10 signal-port 5060 transfer udp primary-proxy-ip1 200.200.200.200
 primary-proxy-port 5060 home-domain huawei sipprofile-index 1
```

Step 7 (Optional) Configure the optional attributes of the SIP interface.

Run the **if-sip attribute optional** command to configure the optional attributes, including the domain name, description, register server uniform resource identifier (URI), phone context, and conference factory URI of the SIP interface.

Step 8 Reset the SIP interface.

```
huawei(config-if-sip-0)#reset
  Are you sure to reset the SIP interface?(y/n)[n]:y
huawei(config-if-sip-0)#quit
```

Step 9 Configure the SIP PSTN user data.

Configure in batches the phone numbers of users 0/3/0-0/3/23 to 83110001-83110024.

NOTE

- To configure the data of a single SIP PSTN user, run the **sippstnuser add** command.
- To configure the data of multiple SIP PSTN users in batches, run the **sippstnuser batadd** command.

```
huawei(config)#esl user
huawei(config-esl-user)#sippstnuser batadd 0/3/0 0/3/23 0 telno 83110001
```

Step 10 Configure call priorities for SIP PSTN users.

```
huawei(config-esl-user)#sippstnuser attribute set 0/3/0 priority cat2
huawei(config-esl-user)#quit
```

Step 11 Configure all the PSTN ports to support polarity reversal.

Configure the physical attributes of the PSTN port to which the users belong to support polarity reversal so that the user supports polarity reversal accounting.

```
huawei(config)#pstnport
huawei(config-pstnport)#pstnport attribute batset 0/3/0 0/3/23 reverse-pole-pulse
enable
huawei(config-pstnport)#quit
```

Step 12 Save the data.

Copyright © Huawei Technologies Co., Ltd.

```
huawei(config)#save
```

----End

11.3.1.9 Configuring Link Aggregation, Congestion Control, and Security Policies

The global configuration of upstream link aggregation and queue scheduling based on priorities ensures service reliability. The global configuration of security policies ensures service security.

Context

Link aggregation provides a higher bandwidth and uplink reliability for optical line terminals (OLTs) by aggregating multiple uplink Ethernet ports to one link aggregation group (LAG). Link aggregation is recommended.

Congestion control places the packets to be sent from a port into multiple queues that are marked with different priorities. Then, the packets are sent based on queue priorities. Congestion control is recommended.

Security policies ensure system, user, and service security.

NOTE

Enable a service security function based on the service type. For details, see **11.2.7 Principle of Security Data Plan**.

Procedure

- Configure link aggregation.

  The following configurations are used as an example to configure link aggregation:

  - Uplink ports 0/19/0 and 0/19/1 are added to a LAG.
  - The two ports send packets upstream based on the packets' source MAC addresses.
  - The LAG works in Link Aggregation Control Protocol (LACP) static aggregation mode.

  ```
  huawei(config)#link-aggregation 0/19 0-1 ingress workmode lacp-static
  ```

- Configure queue scheduling.

  According to quality of service (QoS) planning principles, all packets are scheduled in strict priority (SP) mode and mapped to queues according to the packets' priorities. For details about QoS planning principles, see **11.2.2 Principle of QoS Data Plan**.

  ```
  huawei(config)#queue-scheduler strict-priority
  huawei(config)#cos-queue-map cos0 0 cos4 4 cos5 5 cos6 6
  ```

- Configure system security.
  - Enable deny of service (DoS) anti-attack on both the OLT and optical network units (ONUs).
    1. Run the **security anti-dos enable** command to globally enable DoS anti-attack.
    2. Run the **security anti-dos control-packet policy** command to configure a protocol packet processing policy that will be used when a DoS attack occurs.
    3. Run the **security anti-dos control-packet rate** command to configure the threshold for the rate of sending protocol packets to the CPU.
  - Enable IP address anti-attack on both the OLT and ONUs.

    Run the **security anti-ipattack enable** command to enable IP address anti-attack.

Copyright © Huawei Technologies Co., Ltd.

- Configure user security.
  - Enable MAC address anti-flapping on both the OLT and ONUs.

    Run the **security anti-macduplicate enable** command to enable MAC address anti-flapping.
  - Enable MAC address anti-spoofing on both the OLT and ONUs.
    1. In global config mode, run the **security anti-macspoofing enable** command to globally enable MAC address anti-spoofing.
    2. Enable MAC address anti-spoofing at VLAN level in global config mode or service profile mode:
       a. In global config mode, run the **security anti-macspoofing vlan** command to enable MAC address anti-spoofing.
       b. Perform the following operations to enable MAC address anti-spoofing in service profile mode:
          a. In global config mode, run the **vlan service-profile** command to create a VLAN service profile.
          b. Run the **security anti-macspoofing enable** command to enable MAC address anti-spoofing at VLAN level.
          c. Run the **commit** command to make the profile configuration take effect.
          d. Run the **quit** command to quit the VLAN service profile mode.
          e. Run the **vlan bind service-profile** command to bind the created VLAN service profile to a VLAN.
    3. (Optional) Run the **security anti-macspoofing max-mac-count** command to set the maximum number of MAC addresses that can be bound to a service flow.
    4. (Optional) Run the **security anti-macspoofing exclude** command to configure the types of packets for which MAC address anti-spoofing does not take effect, such as Internet Group Management Protocol (IGMP) packets.
  - Enable IP address anti-spoofing on ONUs.

    IP address anti-spoofing can be enabled or disabled at three levels: global, VLAN, and service port levels. This function takes effect only after it is enabled at the three levels. Among the three levels, IP address anti-spoofing is disabled only at the global level by default.
    1. In global config mode, run the **security anti-ipspoofing enable** command to enable IP address anti-spoofing at the global level.
    2. In VLAN service profile mode, run the **security anti-ipspoofing enable** command to enable IP address anti-spoofing at the VLAN level.
    3. Run the **security anti-ipspoofing service-port** *serviceport-id* **enable** command to enable IP address anti-spoofing at the service port level.
- Configure service security.
  - Enable Dynamic Host Configuration Protocol (DHCP) Option 82 on both the OLT and ONUs. This configuration is recommended for the DHCP-based Internet access service.
    1. Enable DHCP Option 82 on both the OLT and ONUs.

Copyright © Huawei Technologies Co., Ltd.

DHCP Option 82 can be enabled or disabled at four levels: global, port, VLAN, and service port levels. This function takes effect only after it is enabled at the four levels. Among the four levels, DHCP Option 82 is disabled only at the global level by default.

- The global level: In global config mode, run the **dhcp option82** command to enable DHCP Option 82 at the global level.

  When you run this command, select the **enable**, **forward**, or **rebuild** parameter based on site requirements. The three parameters can all enable DHCP Option 82 but provide different packet processing policies on the OLT. For details, see the **dhcp option82** command.

- The port level: In global config mode, run the **dhcp option82 port** or **dhcp option82 board** command to enable DHCP Option 82 at the port level.

- The VLAN level:

  a. In global config mode, run the **vlan service-profile** command to create a VLAN service profile.

  b. Run the **dhcp option82 enable** command to enable DHCP Option 82 at the VLAN level.

  c. Run the **commit** command to make the profile configuration take effect.

  d. Run the **quit** command to quit the VLAN service profile mode.

  e. Run the **vlan bind service-profile** command to bind the created VLAN service profile to a VLAN.

- The service port level: In global config mode, run the **dhcp option82 service-port** command to enable DHCP Option 82 at the service port level.

2. On the OLT, run the **dhcp-option82 permit-forwarding service-port** command with the **enable** parameter selected, to allow ONU DHCP packets to carry Option 82 information.

- Enable Policy Information Transfer Protocol (PITP) on both the OLT and ONUs. This configuration is recommended for the PPPoE-based Internet access service.

  1. Enable PITP on both the OLT and ONUs.

     PITP can be enabled or disabled at four levels: global, port, VLAN, and service port levels. This function takes effect only after it is enabled at the four levels. Among the four levels, PITP is disabled only at the global level by default.

     - The global level: In global config mode, run the **pitp enable pmode**, **pitp forward pmode**, or **pitp rebuild pmode** command to enable PITP at the global level.

       In the preceding commands, the **enable**, **forward**, and **rebuild** parameters can all enable PITP but provide different packet processing policies on the OLT. Select one of them based on site requirements. For details, see the **pitp** command.

     - The port level: In global config mode, run the **pitp port** or **pitp board** command to enable PITP at the port level.

     - The VLAN level:

       a. In global config mode, run the **vlan service-profile** command to create a VLAN service profile.

Copyright © Huawei Technologies Co., Ltd.

b. Run the **pitp enable** command to enable PITP at the VLAN level.
c. Run the **commit** command to make the profile configuration take effect.
d. Run the **quit** command to quit the VLAN service profile mode.
e. Run the **vlan bind service-profile** command to bind the created VLAN service profile to a VLAN.

- The service port level: In global config mode, run the **pitp service-port** command to enable PITP at the service port level.

2. On the OLT, run the **pitp permit-forwarding service-port** command with the **enable** parameter selected, to allow ONU PPPoE packets to carry a vendor tag.

----End

11.3.1.10 Verifying Services

In the Fiber-to-the-building (FTTB) scenario, optical network units (ONUs) are installed in buildings that are far from the central equipment room. ONUs support methods of remote service verification such as Point-to-Point Protocol over Ethernet (PPPoE) dialup emulation and call emulation. Remote site verification eliminates the need to go to site for a second time.

Prerequisites

ONUs are properly connected to upper-layer devices. The broadband remote access server (BRAS) and media gateway controller (MGC)/IP Multimedia Subsystem (IMS) have been configured.

Background Information

Remote Service Verification Method	Function	Remarks
PPPoE emulation dialup	By emulating PPPoE terminal software, an ONU dials up and interacts with the BRAS, to verify the connectivity between the ONT and BRAS.	PPPoE dialup emulation requires a service flow that does not belong to a QinQ VLAN. The user name, password, and authentication mode must be configured on the BRAS before the PPPoE dialup emulation starts. An ONU supports a maximum of one PPPoE dialup emulation.

Copyright © Huawei Technologies Co., Ltd.

Remote Service Verification Method	Function	Remarks
Call emulation	An ONU emulates a call to check whether the voice service configurations are correct. The call emulation function can also be used to locate faults when a voice service is faulty.	● An ONU can emulate a caller or callee in an emulation test. A functional phone is required in the central office where the acceptance personnel is. ● An ONU can emulate the caller and callee simultaneously in an emulation test. No phone is required in the test. ● An ONU supports a maximum of one call emulation.

Data Plan

Item	Data	Remarks
PPPoE dialup emulation parameter	Service flow ID: 101 Emulation timer: 10s	The user name, password, and authentication mode required by the emulation test must be consistent with those configured on the BRAS.
Call emulation parameter	Caller port: 0/3/0 Called port: 0/3/23 Called number: 83110024	When an ONU simultaneously emulates the caller and the callee in an emulation test, retain the parameter settings as default. To query default values, run the **display pots emulational configuration** command.

Procedure

- Verify the Internet access service using PPPoE dialup emulation.
  1. Start an emulation test by running the **simulate dhcp start** command.

```
huawei(config)#pppoe simulate start
  Command:
          pppoe simulate start
 Service-port(index<0-999>):101
 User Name(length<1,65>):user0
 User Password(length<0,16>):*******
 Authentication Mode:
 1. Chap  2. Pap [default 1]:1
 Overtime Time(5-60s)[default 5]:10
```

  2. Query the emulation test information by running the **display pppoe simulate info** command.

Copyright © Huawei Technologies Co., Ltd.

```
huawei(config)#display pppoe simulate info
  PPPoE simulate information is:
  ------------------------------------------------------------------
  Service-port:  101
  User name:     user0
  Current phase: -                    //*Emulation phase
  Result:        Success              //*Emulation result
  Start time:    2011-11-16 15:41:29+08:00
  End time:      2011-11-16 15:41:34+08:00
  Session ID:    591
  User IP:       192.168.50.2
  Gateway IP:    192.168.50.254
  ------------------------------------------------------------------
```

3. Terminate the emulation test by running the **simulate dhcp start** command.

```
huawei(config)#pppoe simulate stop
```

- Verify the voice service using call emulation.
  1. Start an emulation test by running the **ont emulational call** command.

```
huawei(config)#test
huawei(config-test)#pots emulational-call caller-port 0/3/0 callee-port
0/3/23 callee-telno 83110024
```

  2. The ONU outputs the call emulation result after the test is complete.

     The ONU outputs the call emulation result and failure of the cause if the emulation test fails.

```
huawei(config-test)#
  Caller port               :  0/3/0
  Callee port               :  0/3/23
  Test result               :  Test Succeed
```

----End

11.3.2 FTTB/C Networking (xDSL Access, Without HGW)

In the Fiber-to-the-building/curb (FTTB/C) network, an optical network unit (ONU) supports x digital subscriber line (xDSL) and plain old telephone service (POTS) access and provides Internet access and voice over IP (VoIP) services. This topic describes the OLT and ONU configurations required for commissioning Internet access and voice services.

11.3.2.1 Service Requirements and Application Scenario

Generally, Fiber-to-the-building (FTTB) applies to high-density residential areas or commercial centers. Users can access service aggregation nodes using the local area network (LAN) and x digital subscriber line (xDSL). Fiber-to-the-curb (FTTC) applies to low-density residential areas such as villas. xDSL is mainly used in the FTTC scenario because the subscribers are as far as 300 m to 3000 m from the fiber distribution terminal.

Service Requirements

The FTTB/C application scenario only supports Internet access and voice services without multicast demands.

To reuse the existing phone lines and overcome the challenges caused by long distance between ONUs and subscribers, FTTB/C with xDSL access is recommended.

Copyright © Huawei Technologies Co., Ltd.

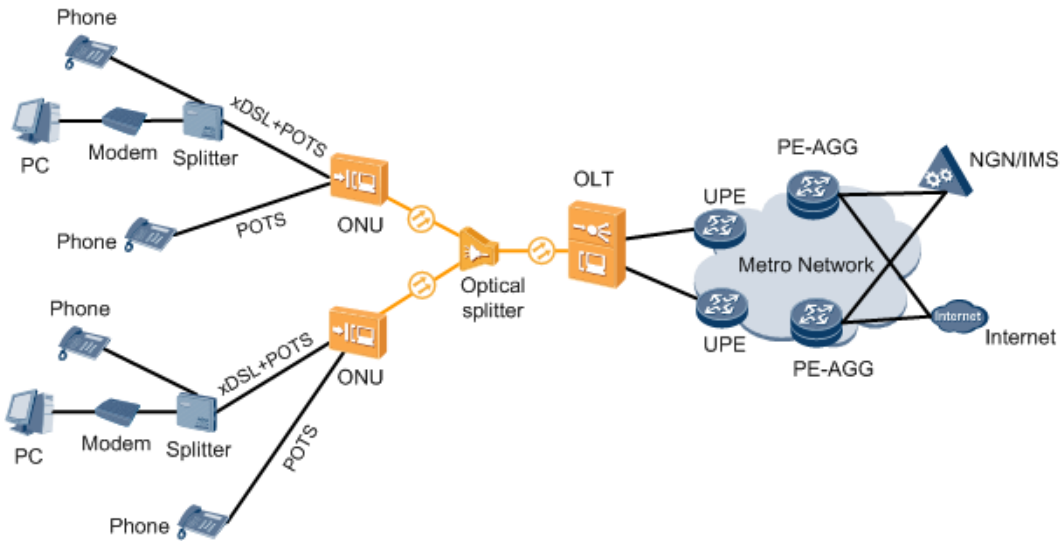
Application Scenario

As shown in **Figure 11-5**, an ONU is deployed in the building corridor, the curb (fiber distribution terminal), or at home through twisted wires.

- Internet access service: A modem at the subscriber's house allows for high-speed Internet access. The subscriber needs to dial up on a computer for authentication because the modem is a Layer 2 device. Each subscriber has a unique account. The broadband remote access server (BRAS) manages and authenticates subscribers.
- Voices service: The voice module built in an ONU can provide voice over IP (VoIP) services.

The ONUs used in this application scenario include MA5616, MA5622A, MA5603T.

Figure 11-5 FTTB/C networking diagram (xDSL)

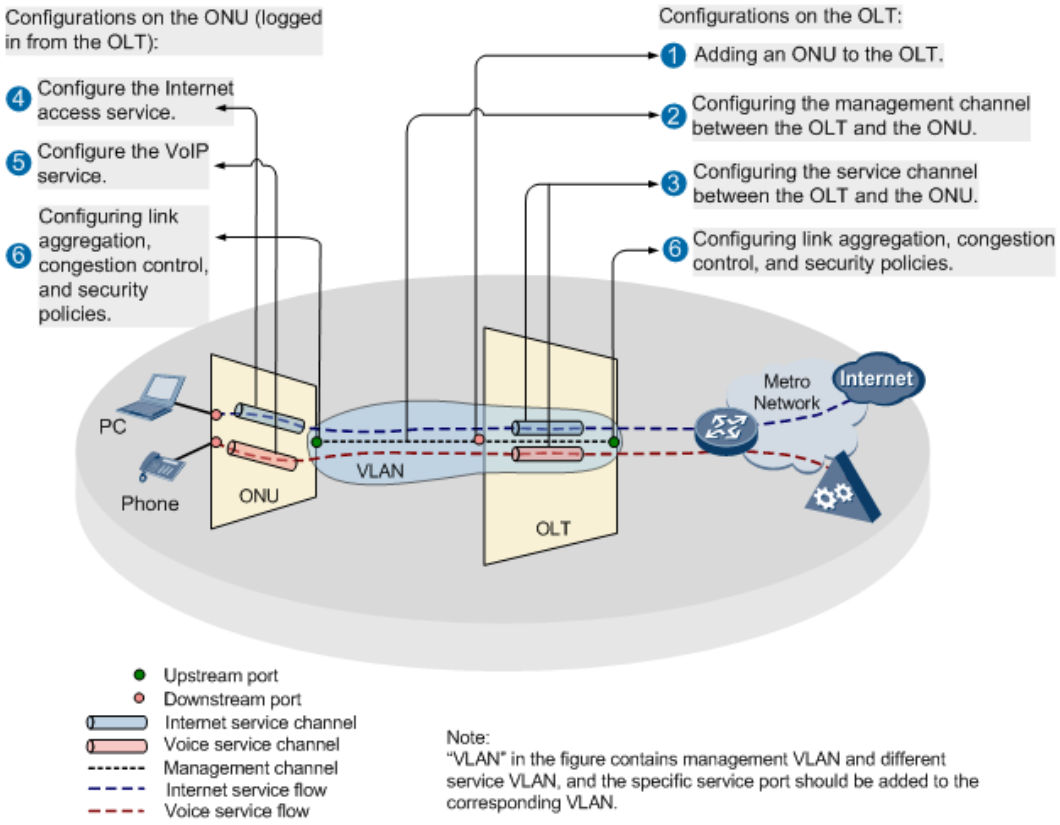


11.3.2.2 Configuration Procedure

Figure 11-6 shows the configuration roadmap diagram in the FTTB and FTTC networking scenarios using xDSL access without HGWs.

Copyright © Huawei Technologies Co., Ltd.

Figure 11-6 Configuration Roadmap Diagram in the FTTB and FTTC Networking Scenarios Using xDSL Access Without HGWs



The following table lists the configuration procedure.

Item	Procedure		Remarks
OLT	**Add an ONU on the OLT.**		Services can be configured for an ONU only after the ONU is successfully added to an OLT.
	Configure the management channel between the OLT and the ONU.		After the inband management channel between the OLT and the ONU is configured and available, you can log in to the ONU from the OLT to configure the ONU.
	Configure the service channel between the OLT and the ONU.	● Configure the Internet access service channel. ● Configure the VoIP service channel.	The ONU provides only the Internet access service and the VoIP service in the FTTB and FTTC network using xDSL access without HGWs. Therefore, you need to create an Internet access service channel and a VoIP service channel on the OLT.

Copyright © Huawei Technologies Co., Ltd.

Item	Procedure		Remarks
ONU	Configure the Internet access service.	**Configure the ADSL2+ Internet access service on the ONU.**	**NOTE** Different ONUs have different ports, including ADSL2+, VDSL2, and VDSL2 vectoring ports, for the Internet access. Select an appropriate configuration method according to the port type.
		Configure the VDSL2 Internet access service on the ONU.	
		(Optional) Configure vectoring on the ONU	
	Configure the VoIP service.	**Configure the H.248 -based VoIP service on the ONU.**	**NOTE** The H.248 and SIP protocols are mutually exclusive for the VoIP service. Only one of them is configured at a time.
		Configure the SIP-based VoIP service on the ONU.	
OLT ONU	**Configure the link aggregation, congestion control, and security policy.**		The global configuration of upstream link aggregation and queue scheduling based on priorities ensures service reliability. The global configuration of security policies ensures service security.
ONU	**Verify the service.**		The ONU provides remote verification methods including PPPoE dialup emulation and call emulation for configuration and commissioning engineers to verify services remotely after service configuration, avoiding a second on-site operation.

11.3.2.3 Adding an ONU to an OLT

Services can be configured for an ONU only after the ONU is successfully added to an OLT.

Context

- When an ONU is added, corresponding profiles need to be bound to the ONU, including the dynamic bandwidth allocation (DBA) profile, line profile, and alarm profile. For details about functions and configuration methods for these profiles, see **Table 11-8**.

Copyright © Huawei Technologies Co., Ltd.

Table 11-8 Introduction to ONU profiles

Profile Type	Function	Command
DBA profile	A DBA profile describes GPON traffic parameters. A T-CONT is bound to a DBA profile for dynamic bandwidth allocation, improving upstream bandwidth utilization.	Query a DBA profile. **display dba-profile** Add a DBA profile. **dba-profile add**
Line profile	A line profile describes binding between the T-CONT and the DBA profile, the QoS mode of the service flow, and mapping between the GEM port and the ONU-side service.	Query a line profile. **display ont-lineprofile** Add a line profile. **ont-lineprofile add**
Alarm profile	An alarm profile contains a series of alarm threshold parameters that are used for performance measurement and monitoring of the activated ONT lines.	Query an alarm profile. **display gpon alarm-profile** Add an alarm profile. **gpon alarm-profile add**

- An ONU can be added in two modes. Select either mode as required.

Mode	Usage Scenario	Command
Add an ONU offline.	The ONU password or serial number (SN) is obtained.	Run the **ont add** command to add an ONU.
Online confirm an ONU.	Both the ONU password and SN are not obtained.	In the GPON mode, run the **port ont-auto-find** command to enable the ONU auto-discovery function of a GPON port and then run the **ont confirm** command to add an ONU.

Data plan

Table 11-9 Data plan

Item	Data
DBA profile	Profile name: fttb_dba Profile type: type3 Assured bandwidth: 8 Mbit/s Maximum bandwidth: 20 Mbit/s

Copyright © Huawei Technologies Co., Ltd.

Item	Data
Line profile	Profile name: fttb(c) Profile ID: 10 T-CONT ID: 4 GEM port ID for management service: 11 GEM port ID for Internet access service: 12 GEM port ID for VoIP service: 13
Network topology data	PON port: 0/2/1 ONT ID: 1

Procedure

Step 1 Configure GPON ONU profiles.

1. Configure a DBA profile.

   ```
   huawei(config)#dba-profile add profile-name fttb_dba type3 assure 8192 max 20480
   ```

2. Configure an ONU line profile.

   a. Add GPON ONU line profile 10 fttb(c).

   ```
   huawei(config)#ont-lineprofile gpon profile-id 10 profile-name fttb(c)
   ```

   NOTE

   The ID of the line profile to be created must not exist in the system and the line profile must be created according to the data plan. In this example, line profile 10 is used.

   b. In the line profile mode, bind T-CONT 4 to DBA profile fttb_dba.

   ```
   huawei(config-gpon-lineprofile-10)#tcont 4 dba-profile-name fttb_dba
   ```

   c. In the line profile mode, bind the GEM port to the T-CONT.

   - Add GEM port 11 to carry management service flows.
   - Add GEM port 12 to carry Internet access service flows.
   - Add GEM port 13 to carry VoIP service flows.

   Bind GEM ports 11, 12, and 13 to T-CONT 4. In configuring, QoS policies for various service flows also need to be configured. For details about QoS data plan, see **11.2.2 Principle of QoS Data Plan**.

   ```
   huawei(config-gpon-lineprofile-10)#gem add 11 eth tcont 4 cascade on
   huawei(config-gpon-lineprofile-10)#gem add 12 eth tcont 4 cascade on
   huawei(config-gpon-lineprofile-10)#gem add 13 eth tcont 4 cascade on
   ```

   d. Configure mapping between the GEM port and the ONU-side service.

   Set the mode for mapping the GEM port to the ONU-side service to the VLAN mapping mode (default). Map management service flows (the CVLAN ID is 8) to GEM port 11, Internet access service flows (the CVLAN ID is 1001) to GEM port 12, and VoIP service flows (the CVLAN ID is 200) to GEM port 13.

   ```
   huawei(config-gpon-lineprofile-10)#gem mapping 11 0 vlan 8
   huawei(config-gpon-lineprofile-10)#gem mapping 12 1 vlan 1001
   huawei(config-gpon-lineprofile-10)#gem mapping 13 2 vlan 200
   ```


Copyright © Huawei Technologies Co., Ltd.

e. After the configuration is completed, run the **commit** command to make the configured parameters take effect.

```
huawei(config-gpon-lineprofile-10)#commit
huawei(config-gpon-lineprofile-10)#quit
```

3. (Optional) Add an alarm profile.
   - The ID of the default GPON alarm profile is 1. The thresholds for all the alarm parameters in the default alarm profile are 0, which indicates that no alarm is generated.
   - In this example, the default alarm profile is used and therefore the configuration of the alarm profile is not required.

Step 2 Add an ONU to an OLT.

Assume that the ID of GPON port 0/2/1 is 1, SN is 32303131B39FD641, management mode is SNMP, and the bound line profile is fttb(c). Connect the ONU to such a GPON port through the optical splitter.

There are two modes to add an ONT: add an ONT offline and confirm an automatically discovered ONU.

- Add an ONU offline.

```
huawei(config)#interface gpon 0/2
huawei(config-if-gpon-0/2)#ont add 1 ontid 1 sn-auth 32303131B39FD641
snmp ont-lineprofile-name fttb(c)
```

- Confirm an automatically discovered ONU.

```
huawei(config)#interface gpon 0/2
huawei(config-if-gpon-0/2)#port 1 ont-auto-find enable
huawei(config-if-gpon-0/2)#display ont autofind 1
huawei(config-if-gpon-0/2)#ont confirm 1 ontid 1 sn-auth 32303131B39FD641
snmp ont-lineprofile-name fttb(c)
```

1. (Optional) Bind the alarm profile to the ONU.

   By default, alarm profile 1 automatically bound to an ONU. A non-default alarm profile is bound manually only when the default one does not meet the requirement.

   In this example, default alarm profile 1 is used and therefore the configuration of the alarm profile is not required.

Step 3 Check the ONU status.

After an ONU is added, run the **display ont info** command to query the current status of the ONU. Ensure that **Config flag** of the ONU is **active**, **Run State** is **online**, and **Config state** is **normal**.

```
huawei(config-if-gpon-0/2)#display ont info 1 1
  ------------------------------------------------------------------------
  F/S/P                : 0/2/1
  ONT-ID               : 1
  Control flag         : active    //The ONU is activated.
  Run state            : online    //The ONU is online.
  Config state         : normal    //The ONU configurations are recovered
normally.
...//The rest of the response information is not provided here.
huawei(config-if-gpon-0/2)#quit
```

----End

Follow-up Procedure

When **Config state** is **failed**, **Run state** is **offline**, or **Match state** is **mismatch**:

Copyright © Huawei Technologies Co., Ltd.

- If **Control flag** is **deactive**, run the **ont active** command in GPON mode to activate the ONU.
- If **Run state** is **offline**, a physical line may be broken or the optical module may be damaged. Check the line and the optical module.
- If **Config state** is **failed**, the configured ONU capability exceeds the actual ONU capability. In this case, run the **display ont failed-configuration** command in the diagnose mode to check the failed configuration item and the failure cause. Then, rectify the fault accordingly.
- If the ONU does not match, that is, **Match state** is **mismatch**, the port types and number of ports undermatch the actual port types and number of ports supported by the ONU. In this case, run the **display ont capability** command to query the actual capability of the ONU, and then select one of the following modes to modify the ONU configuration:
  - Create a proper ONU profile according to the actual capability of the ONU, and then run the **ont modify** command to modify the configuration data of the ONU.
  - Modify the ONU profile according to the actual capability of the ONU and save the modification. Then, the ONU automatically recovers the configuration successfully.

11.3.2.4 Configuring the Management Channel Between the OLT and the ONU

After the inband management channel between the OLT and the ONU is configured and available, you can log in to the ONU from the OLT to configure the ONU.

Data plan

Item	Data	Remarks
Management VLAN and management IP address on the OLT side	Management VLAN ID: 8 Management VLAN type: smart VLAN Inband management IP address: 192.168.50.1/24	To configure the MDU from the OLT by remote logging in to the MDU, the management VLAN of the OLT and that of the MDU must be the same, and the management IP address of the OLT and that of the MDU must be in the same network segment.
Management VLAN and management IP address on the ONU side	Management VLAN ID: 8 Management VLAN type: smart VLAN Inband management IP address: 192.168.50.2/24	

Procedure

Step 1 Configure the inband management VLAN and IP address of the OLT.

Configure the inband management VLAN to 8, VLAN priority to 6, and the IP address to 192.168.50.1/24.

```
huawei(config)#vlan 8 smart
huawei(config)#port vlan 8 0/19 0
huawei(config)#vlan priority 8 6
huawei(config)#interface vlanif 8
```


Copyright © Huawei Technologies Co., Ltd.

```
huawei(config-if-vlanif8)#ip address 192.168.50.1 24
huawei(config-if-vlanif8)#quit
```

Step 2 Configure the inband management VLAN and IP address of the ONU.

Configure the static IP address of the ONU to 192.168.50.2/24, gateway to 192.168.50.254, and the management VLAN ID to 8 (the same as the management VLAN of the OLT).

```
huawei(config)#interface gpon 0/2
huawei(config-if-gpon-0/2)#ont ipconfig 1 1 static ip-address 192.168.50.2 mask
255.255.255.0 gateway
192.168.50.254 vlan 8
huawei(config-if-gpon-0/2)#quit
```

Step 3 Configure an inband management service port.

Configure the management service port ID to 1, management VLAN ID to 8, GEM port ID to 11, and user-side VLAN ID to 8. The OLT does not limit inband management service flows. Therefore, it is recommended that you use default traffic profile 6.

```
huawei(config)#service-port 1 vlan 8 gpon 0/2/1 ont 1 gemport 11 multi-service
user-vlan 8 rx-cttr 6 tx-cttr 6
```

Step 4 Confirm that the management channel between the OLT and the ONU is available.

- On the OLT, run the **ping** ***192.168.50.2*** command to check the connectivity between the OLT and the ONU. The ICMP ECHO-REPLY packet from the ONU should be received.
- On the OLT, you can remote log in to the ONU to perform the configuration.

----End

11.3.2.5 Configuring the Service Channel Between the OLT and the ONU

Various service flows can be configured on the OLT for different services so that service packets on the ONU can be forwarded at Layer 2 according to the planned VLAN and forwarding policies.

Context

Service flows can be added in two modes, as described in **Table 11-10**. Select either mode as required.

Table 11-10 Adding service flows

Mode	Command	Remarks
Add service flows one by one.	**service-port**	-
Add service flows in batches.	**multi-service-port**	You need to specify the **ontid** + **gemindex** to identify a service flow and ensure that the number of GEM ports is the same as the number of VLANs on the user side.

Copyright © Huawei Technologies Co., Ltd.

Data plan

Item	Data	Remarks
Internet access service	OLT VLAN ID: ● CVLAN ID: 256 x GPON port ID + 32 x Split ratio x (Splitter port ID - 1) + ONU port ID + 1 ● SVLAN: VLAN ID 100 and attribute stacking Upstream VLANs of the ONU: 1001-1016 Service flow ID: 101	Assume that the split ratio of the optical splitter is 1:32, the ONU is connected to port 1 on the optical splitter using the optical cable, and the user PC is connected to port 1 on the ONU. In this case, the inner VLAN is 258 according to the formula for calculating the inner VLAN. For details about the data plan, see **11.2.3 Principle of Internet Access Service Data Plan**.
VoIP service	OLT VLAN ID (VLAN transparently transmitting the ONU service): 200 ONU VLAN ID: 200 Service flow ID: 201	For details about the data plan, see **11.2.5 Principle of VoIP Service Data Plan**.

Procedure

- Configure the channel for the Internet access service.
  1. Configure the service VLAN and add the upstream port to this VLAN.

     Configure the SVLAN ID to 100, VLAN type to smart VLAN, and VLAN attribute to stacking. Add upstream port 0/19/0 to VLAN 100.

     ```
     huawei(config)#vlan 100 smart
     huawei(config)#vlan attrib 100 stacking
     huawei(config)#port vlan 100 0/19 0
     ```

  2. Configure the corresponding traffic profile.

     The 802.1p priority for the Internet access service is 0 and the traffic profile is unlimited. You can run the **display traffic table ip** command to query the traffic profile in the system. Use traffic profile 6.

     ```
     huawei(config)#display traffic table ip from-index 0
     ```

  3. Configure service flows to receive and transparently transmits the Internet access service from the ONU.

     According to the data plan,

     - For the OLT: The SVLAN ID is 100, inner VLAN ID is 258. The user-side VLAN ID of the OLT is the same as the upstream VLAN ID of the ONU, that is, 1001. The Internet access service uses GEM port 12.
     - For the ONU: The upstream VLAN ID is 1001.

     ```
     huawei(config)#service-port 101 vlan 100 gpon 0/2/1 ont 1 gemport 12 multi-service
     ```


Copyright © Huawei Technologies Co., Ltd.

```
user-vlan 1001 tag-transform translate-and-add inner-vlan 258 rx-cttr 6 tx-cttr 6
```

- Configure the channel for the VoIP service.
  1. Configure the service VLAN and add the upstream port to this VLAN.

     Configure the SVLAN ID to 200 and VLAN type to smart VLAN. Add upstream port 0/19/0 to VLAN 200.

     ```
     huawei(config)#vlan 200 smart
     huawei(config)#port vlan 200 0/19 0
     ```

  2. Configure the corresponding traffic profile.

     The 802.1p priority of the VoIP service is 5 and the traffic profile is unlimited. You can run the **display traffic table ip** command to query the traffic profile in the system. If the existing traffic profile does not meet data plan requirements, a new traffic profile is required.

     New traffic profile 9 is added. In the command execution, *priority-policy* is **local-setting**, which indicates that service packets are scheduled by the priority specified in the traffic profile.

     ```
     huawei(config)#traffic table ip index 9 cir off priority 5 priority-policy local-setting
     ```

  3. Configure service flows to receive and transparently transmits the VoIP service from the ONU.

     According to the data plan,

     - For the OLT: The SVLAN ID is 200. The user-side VLAN ID of the OLT is the same as the upstream VLAN ID of the ONU, that is, 200. The VoIP service uses GEM port 13.
     - For the ONU: The upstream VLAN ID is 200.

     ```
     huawei(config)#service-port 201 vlan 200 gpon 0/2/1 ont 1 gemport 13 multi-service
     user-vlan 200 rx-cttr 9 tx-cttr 9
     ```

----End

11.3.2.6 Configuring the Internet Access Service (ADSL2+ Access, on the ONU)

This topic describes how to configure the Internet access service for home gateway (HGW) users on an optical network unit (ONU) when HGWs are connected upstream to the ONU in ADSL2 + mode.

Context

ADSL2+ ports working in normal mode (that is, RFC 2662 mode) need to bind an ADSL2+ line profile and an ADSL2+ alarm profile. For the functions and configurations of each profile, see **Table 11-11**.

Copyright © Huawei Technologies Co., Ltd.

Table 11-11 ADSL2+ profile

Profile Type	Function	Configuration
ADSL2+ line profile	An ADSL2+ line profile provides the following parameters: ● ADSL/ADSL2+ working mode ● Channel mode ● Upstream/Downstream line rate ● Upstream/Downstream interleave depth ● Noise margin When an ADSL2+ port is activated, the central office (CO) and the customer premises equipment (CPE) negotiate based on the parameters configured in the ADSL2+ line profile, to determine whether the ADSL2+ port can work in the normal state in these conditions.	The system has four default profiles (profile 1, profile 1022, profile 1023, and profile 1024) for activation of ADSL2+ ports in different conditions. ● Profile 1 is used for activation of common ADSL ports. ● Profile 1022 is used for fast activation of ADSL ports. ● Profile 1023 is used for long-reach activation of existing ADSL ports. ● Profile 1024 is used for activation of ports on ADSL2+ boards. Commands: ● To query: **display adsl line-profile** ● To add: **adsl line-profile add** or **adsl line-profile quickadd**
ADSL2+ alarm profile	Values to be configured in an ADSL2 + line alarm profile are thresholds within any 15 minutes. When the statistics of an item reach the threshold, the system informs the device of the event and sends alarms to the NMS.	Commands: ● To query: **display adsl alarm-profile** ● To add: **adsl alarm-profile add** or **adsl alarm-profile quickadd**

Data Plan

The following table provides key information about the Internet access service (ADSL2+ access).

Item	Data	Remarks
Traffic profile	ID: 8 CIR: 4 Mbit/s VLAN priority: 0 Downstream priority policy: local-setting	A traffic profile implements rate-limiting.
VPI/VCI of ADSL2+ users	VPI: 0 VCI: 35	Internet service providers (ISPs) provide VPI/VCI information.

Copyright © Huawei Technologies Co., Ltd.

Item	Data	Remarks
ADSL2+ line profile	ID: 1024 (default); key parameters: ● Working mode: full compatibility ● Channel working mode: interleaved ● Maximum upstream/ downstream rate (kbit/s): 24544/1024	A traffic profile or an ADSL2+ line profile can implement rate-limiting on ADSL2+ ports. This example uses a default traffic profile.
ADSL2+ alarm profile	ID: 1 (default)	The system does not check whether parameter thresholds are crossed and so does not report alarms.

Procedure

Step 1 Log in to the ONU to perform the configuration.

You can remote log in to the ONU from the OLT to perform the configuration. User name: **root** (default). Password: **mduadmin** (default).

Step 2 Configure a traffic profile.

You can run the **display traffic table ip** command to query the traffic profiles existing in the system. If the traffic profiles existing in the system do not meet the requirements, you need to run the **traffic table ip** command to add a traffic profile.

Add traffic profile 8 and set the committed information rate (CIR) to 4 Mbit/s. The priority for upstream packets is 0, and downstream packets are scheduled based on the priority specified in the traffic profile.

```
huawei(config)#traffic table ip index 8 cir 4096 priority 0 priority-policy local-setting
```

Step 3 Create service VLANs.

Create service VLANs 1001-1016 in batches whose type is smart and attribute is common (the service VLAN IDs must be consistent with the user VLAN IDs of the OLT). Add the service VLANs to upstream port 0/0/1.

```
huawei(config)#vlan 1001-1016 smart
huawei(config)#port vlan 1001-1016 0/0 1
```

Step 4 Add a service port.

Assume that the VPI/VCI of users is 0/35 and the VLAN ID is 1001. Add a service port as follows:

```
   //Create service port 101, bind port 0/2/0 to it, set VPI/VCI to 0/35, and bind traffic profile 8 to the user VLAN./
huawei(config)#service-port 101 vlan 1001 adsl 0/2/0 vpi 0 vci 35 multi-service user-vlan untagged rx-cttr 8 tx-cttr 8
```

Step 5 (Optional) Configure an ADSL2+ line profile.

- Configure an ADSL2+ line profile only when the default one does not meet requirements.

Copyright © Huawei Technologies Co., Ltd.

- This example uses the default ADSL2+ line profile (ID: 1024).

Step 6 (Optional) Configure an ADSL2+ alarm profile.

This example uses the default ADSL2+ alarm profile (ID: 1).

Step 7 Bind an ADSL2+ line profile and an ADSL2+ alarm profile, and activate the ADSL2+ port.

For example, bind ADSL2+ line profile 1024 and ADSL2+ alarm profile 1, and activate ADSL2+ port 0/2/0.

```
huawei(config)#interface adsl 0/2
huawei(config-if-adsl-0/2)#deactivate 0
huawei(config-if-adsl-0/2)#alarm-config 0 1
huawei(config-if-adsl-0/2)#activate 0 profile-index 1024
```

----End

11.3.2.7 Configuring the Internet Access Service (VDSL2 Access, on the ONU)

This topic describes how to configure the Internet access service for home gateway (HGW) users on an optical network unit (ONU) when HGWs are connected upstream to the ONU in VDSL2 mode.

Context

VDSL2 ports working in normal mode (that is, TR129 mode) need to bind the VDSL2 line template and VDSL2 alarm template. For the functions and configurations of each profile, see **Table 11-12**.

Table 11-12 VDSL2 template

Template Type	Function	Configuration
VDSL2 line template	A VDSL2 line template consists of a VDSL2 line profile and a VDSL2 channel profile. When a VDSL2 port is activated, the central office (CO) and the customer premises equipment (CPE) negotiate based on the parameters configured in the VDSL2 line template, to determine whether the VDSL2 port can work in the normal state in these conditions.	The system has one default VDSL2 line template (template 1), which is used for activation of common VDSL2 ports. ● To query: **display vdsl line-template** ● To add: **vdsl line-template add** or **vdsl line-template quickadd**
	A VDSL2 line profile provides the following parameters: line transmission mode, adaptation mode of upstream/downstream transmit rates, signal-to-noise ratio (SNR) margin, upstream power back-off (UPBO), and downstream power back-off (DPBO).	● To query: **display vdsl line-profile** ● To add: **vdsl line-profile add** or **vdsl line-profile quickadd**

Copyright © Huawei Technologies Co., Ltd.

Template Type	Function	Configuration
	A VDSL2 channel profile provides the following parameters: data channel mode, minimum impulse noise protection, interleaved delay parameters, rate parameters, retransmission at the physical layer, erasure decoding, and G.998.4 retransmission.	● To query: **display vdsl channel-template** ● To add: **vdsl channel-template add** or **vdsl channel-profile quickadd**
VDSL2 alarm template	A VDSL2 alarm template consists of a VDSL2 line alarm profile and a VDSL2 channel alarm profile. Values to be configured in a VDSL2 alarm template are thresholds within any 15 minutes. When the statistics of an item reach the threshold, the system informs the device of the event, and sends alarms to the NMS.	The system has one default VDSL2 alarm template (template 1). ● To query: **display vdsl alarm-template** ● To add: **vdsl alarm-template add** or **vdsl alarm-template quickadd**
	A VDSL2 line alarm profile provides the following parameters for COs and CPEs: ● Forward error check seconds (FECS) ● Errored seconds (ES) ● Severely errored seconds (SES) ● Loss of signal seconds (LOSS) ● Unavailable seconds (UAS) ● Low error-free throughput rate (LEFTR) defect seconds	● To query: **display vdsl alarm-profile** ● To add: **vdsl alarm-profile add** or **vdsl alarm-profile quickadd**
	A VDSL2 channel alarm profile provides the following parameters for COs and CPEs: ● Coding violations counts (CVC) ● Corrected blocks counts (CBC)	● To query: **display vdsl channel-alarm-profile** ● To add: **vdsl channel-alarm-profile add** or **vdsl channel-alarm-profile quickadd**

Data Plan

Table 11-13 provides key information about the Internet access service (VDSL2 access).

Copyright © Huawei Technologies Co., Ltd.

Table 11-13 Key information about the Internet access service (VDSL2 access)

Item	Data	Remarks
Traffic profile	ID: 8 CIR: 4 Mbit/s VLAN priority: 0 Downstream priority policy: local-setting	A traffic profile implements rate-limiting.
VDSL2 line mode	PTM	There are two VDSL line modes: ATM mode and PTM mode. ● ATM mode: ATM cells are transmitted in channels. This mode is compatible with the ADSL2+ mode. ● PTM mode: IP cells are transmitted in channels. This mode is incompatible with the ADSL2+ mode. This example assumes the PTM mode.
VDSL2 line template	Line profile ID: 1 (default)	A traffic profile or a VDSL2 line template can implement rate-limiting on VDSL2 ports. This example uses a default traffic profile.
	Channel profile ID: 1 (default)	
	Line template ID: 1 (default)	
VDSL2 alarm template	Line alarm profile ID: 1 (default)	The system does not check whether parameter thresholds are crossed and so does not report alarms.
	Channel alarm profile ID: 1 (default)	
	Alarm template ID: 1 (default)	

Procedure

Step 1 Log in to the ONU to perform the configuration.

You can remote log in to the ONU from the OLT to perform the configuration. User name: **root** (default). Password: **mduadmin** (default).

Step 2 Configure a traffic profile.

You can run the **display traffic table ip** command to query the traffic profiles existing in the system. If the traffic profiles existing in the system do not meet the requirements, you need to run the **traffic table ip** command to add a traffic profile.

Add traffic profile 8 and set the committed information rate (CIR) to 4 Mbit/s. The priority for upstream packets is 0, and downstream packets are scheduled based on the priority specified in the traffic profile.

Copyright © Huawei Technologies Co., Ltd.

```
huawei(config)#traffic table ip index 8 cir 4096 priority 0 priority-policy local-setting
```

Step 3 Create service VLANs.

Create service VLANs 1001-1016 in batches whose type is smart and attribute is common (the service VLAN IDs must be consistent with the user VLAN IDs of the OLT). Add the service VLANs to upstream port 0/0/1.

```
huawei(config)#vlan 1001-1016 smart
huawei(config)#port vlan 1001-1016 0/0 1
```

Step 4 Add a service port.

Assume that the VDSL2 path mode is PTM mode, VLAN ID is 1001, port is 0/1/0, packets from the user VLAN are untagged, and service flow ID is 101. Add a service port as follows:

```
huawei(config)#service-port 101 vlan 1001 vdsl mode ptm 0/1/0 multi-service user-vlan untagged rx-cttr 8 tx-cttr 8
```

Step 5 Configure a VDSL2 line template.

This example uses the default VDSL2 line template (ID: 1).

Step 6 Configure a VDSL2 alarm template.

This example uses the default VDSL2 alarm template (ID: 1).

Step 7 Bind a VDSL2 line template and a VDSL2 alarm template, and activate the VDSL2 port.

For example, bind VDSL2 line template 1 and VDSL2 alarm template 1, and activate VDSL2 port 0/1/0.

```
huawei(config)#interface vdsl 0/1
huawei(config-if-vdsl-0/1)#deactivate 0
huawei(config-if-vdsl-0/1)#alarm-config 0 1
huawei(config-if-vdsl-0/1)#activate 0 template-index 1
```

----End

11.3.2.8 (Optional) Configuring Vectoring

Vectoring configurations on VDSL2 lines cancel the far-end crosstalk (FEXT) of VDSL2 lines to improve the line rate.

Context

For MA5623A/MA5616, when configuring vectoring, learn configuration item functions and configuration methods beforehand by referring to **Table 11-14**.

Copyright © Huawei Technologies Co., Ltd.

Table 11-14 Vectoring configuration items

Item	Function	Description	Commands
Global band plan	In the vectoring algorithm, the system requires that the upstream band and downstream band are separate from each other. Therefore, the band plan must be globally configured.	● The band plan can be globally configured only when vectoring is globally enabled. ● After vectoring is globally enabled, if the band plan configured for the line profile is incompatible with the band plan globally configured for vectoring and the upstream band plan and downstream band plan are not separate from each other, the port cannot be activated.	xdsl vectoring bandplan-type
Global vectoring configurations	Vectoring configurations take effect only when vectoring is globally enabled.	● Before enabling vectoring, globally configure the band plan. **NOTE** Services in a vectoring group port are interrupted when the vectoring function is enabled or disabled.	xdsl vectoring

Copyright © Huawei Technologies Co., Ltd.

Item	Function	Description	Commands
Vectoring profile	Configure the function of canceling the upstream and downstream crosstalk in the vectoring profile. After binding the configured vectoring profile to the ports, the system implements the vectoring algorithm on the ports in the vectoring group based on profile configurations.	By default, all ports are bound to vectoring profile 1. Default value: ● Upstream crosstalk cancelation: enable ● Downstream crosstalk cancelation: enable	Query a vectoring profile: display xdsl vectoring-profile
Policy for controlling frequent online and offline on ports	The Vectoring algorithm is executed every time a port in a Vectoring group goes online or offline. To prevent adverse impact on system functions due to long-term running Vectoring tasks caused by frequent online and offline on a port, set the policy for controlling frequent online and offline on ports based on site requirements.	By default, the policy for controlling frequent online and offline is set to limit.	xdsl frequently-retrain-control
Vectoring crosstalk matrix	The vectoring crosstalk matrix refers to crosstalk on a port in a vectoring group from other ports in the same vectoring group.	Before querying information about the vectoring crosstalk matrix, ensure that the global vectoring function is enabled and the specified port is in a vectoring group and activated.	display xdsl vectoring crosstalk-coupling-matrix

Copyright © Huawei Technologies Co., Ltd.

Item	Function	Description	Commands
Policy for activating a legacy customer premises equipment (CPE)	A legacy CPE is a VDSL2 CPE (supporting G.993.2, not G.993.5) that does not support Vectoring. If such a CPE is activated in G.993.2 mode in the Vectoring system, the crosstalk impact on other lines cannot be canceled, causing the Vectoring system performance to deteriorate. To minimize the impact, set the activation policy of a legacy CPE based on site requirements.	By default, the policy for activating a legacy CPE is set to limit. ● **no-limit**: The Vectoring legacy CPE is activated in common VDSL2 mode (G.993.2 mode), or non-Vectoring mode, in which the Vectoring system performance is affected. This mode is used in the Vectoring initial phase when a large number of CPEs need to be upgraded or replaced and the Vectoring performance are not concerned. ● **limit**: The Vectoring legacy CPE is activated in common VDSL2 mode but the line PSD is automatically shaped so that the CPE can be activated at a low VDSL2 rate, preventing crosstalk on other lines. This mode is used in Vectoring medium phase when some CPEs have not been upgrade or replaced. ● **force-friendly-ds-limit-us**: **force friendly** is used in the downstream	xdsl vectoring legacy-cpe activate-policy

Copyright © Huawei Technologies Co., Ltd.

Item	Function	Description	Commands
		direction and PSD automatic shaping is used in the upstream direction. ● **force-friendly-ds-no-limit-us**: **force friendly** is used in the downstream direction and no restriction is used in the upstream direction. ● **block**: The Vectoring legacy CPE cannot be activated in common VDSL2 mode. This mode is used in Vectoring mature phase when its performance is concerned and unnecessary crosstalk must be prevented.	

For MA5603T, when configuring vectoring, learn configuration item functions and configuration methods beforehand by referring to **Table 11-15**.

Copyright © Huawei Technologies Co., Ltd.

Table 11-15 Vectoring configuration items

Item	Function	Description	Commands
Global band plan	In the vectoring algorithm, the system requires that the upstream band and downstream band are separate from each other. Therefore, the band plan must be globally configured.	● The band plan can be globally configured only when vectoring is globally enabled. ● After vectoring is globally enabled, if the band plan configured for the line profile is incompatible with the band plan globally configured for vectoring and the upstream band plan and downstream band plan are not separate from each other, the port cannot be activated.	xdsl vectoring bandplan-type
Global vectoring configurations	Vectoring configurations take effect only when vectoring is globally enabled.	● Vectoring can be globally enabled only when devices are configured with VP boards. ● Before enabling vectoring, globally configure the band plan. **NOTE** Services in a vectoring group port are interrupted when the vectoring function is enabled or disabled.	xdsl vectoring

Copyright © Huawei Technologies Co., Ltd.

Item	Function	Description	Commands
Vectoring profile	Configure the function of canceling the upstream and downstream crosstalk in the vectoring profile. After binding the configured vectoring profile to the ports, the system implements the vectoring algorithm on the ports in the vectoring group based on profile configurations.	By default, all ports are bound to vectoring profile 1. Default value: ● Upstream crosstalk cancelation: enable ● Downstream crosstalk cancelation: enable	Commands: ● Add a vectoring profile: xdsl vectoring-profile add ● Modify a vectoring profile: xdsl vectoring-profile modify ● Delete a vectoring profile: xdsl vectoring-profile delete ● Query a vectoring profile: display xdsl vectoring-profile ● Bind a vectoring profile to the port: vectoring-config (VDSL mode)
Policy for controlling frequent online and offline on ports	The Vectoring algorithm is executed every time a port in a Vectoring group goes online or offline. To prevent adverse impact on system functions due to long-term running Vectoring tasks caused by frequent online and offline on a port, set the policy for controlling frequent online and offline on ports based on site requirements.	By default, the policy for controlling frequent online and offline is set to limit.	xdsl frequently-retrain-control

Copyright © Huawei Technologies Co., Ltd.

Item	Function	Description	Commands
Vectoring crosstalk matrix	The vectoring crosstalk matrix refers to crosstalk on a port in a vectoring group from other ports in the same vectoring group.	Before querying information about the vectoring crosstalk matrix, ensure that the global vectoring function is enabled and the specified port is in a vectoring group and activated.	display xdsl vectoring crosstalk-coupling-matrix

Copyright © Huawei Technologies Co., Ltd.

Item	Function	Description	Commands
Policy for activating a legacy customer premises equipment (CPE)	A legacy CPE is a VDSL2 CPE (supporting G. 993.2, not G. 993.5) that does not support Vectoring. If such a CPE is activated in G.993.2 mode in the Vectoring system, the crosstalk impact on other lines cannot be canceled, causing the Vectoring system performance to deteriorate. To minimize the impact, set the activation policy of a legacy CPE based on site requirements.	By default, the policy for activating a legacy CPE is set to limit. ● **no-limit**: The Vectoring legacy CPE is activated in common VDSL2 mode (G.993.2 mode), or non-Vectoring mode, in which the Vectoring system performance is affected. This mode is used in the Vectoring initial phase when a large number of CPEs need to be upgraded or replaced and the Vectoring performance are not concerned. ● **limit**: The Vectoring legacy CPE is activated in common VDSL2 mode but the line PSD is automatically shaped so that the CPE can be activated at a low VDSL2 rate, preventing crosstalk on other lines. This mode is used in Vectoring medium phase when some CPEs have not been upgrade or replaced. ● **force-friendly-ds-limit-us**: **force friendly** is used in the downstream	xdsl vectoring legacy-cpe activate-policy

Copyright © Huawei Technologies Co., Ltd.

Item	Function	Description	Commands
		direction and PSD automatic shaping is used in the upstream direction. ● **force-friendly-ds-no-limit-us**: **force friendly** is used in the downstream direction and no restriction is used in the upstream direction. ● **block**: The Vectoring legacy CPE cannot be activated in common VDSL2 mode. This mode is used in Vectoring mature phase when its performance is concerned and unnecessary crosstalk must be prevented.	

Data Plan

The **Table 11-16** lists key parameters of vectoring configurations.

Table 11-16 Key parameters of vectoring configurations

Item	Data	Description
Global vectoring configurations	enable	-
Global band plan	● Band plan type: 998ade ● USO type: type-a	-
Policy for activating a legacy customer premises equipment (CPE)	no-limit	The policy for activating a vectoring legacy CPE is configured as **no-limit** at the initial stage of vectoring application.

Copyright © Huawei Technologies Co., Ltd.

Item	Data	Description
Policy for controlling frequent online and offline on ports	no-limit	-
Vectoring group	Group ID: 1	All ports are added to the default vectoring group 1.
Vectoring profile	For the MA5623A/MA5616: Profile ID: 1 The upstream/ downstream crosstalk cancelation function in default Profile 1 are as follows: ● Upstream crosstalk cancelation: enable ● Downstream crosstalk cancelation: enable	-
	For MA5603T: ● Profile name: huawei ● Upstream crosstalk cancelation: enable ● Downstream crosstalk cancelation: enable ● The port to which a vectoring profile is bound: all ports on the0/1 board.	

NOTE

The Vectoring is configured on the ONU, and the configuration between the MA5623A/MA5616 and MA5603T is a little different, Here gives the configuring steps of MA5623A/MA5616 and MA5603T respectively.

Procedure

- Configuration procedure for the MA5623A/MA5616:
  1. Log in to the ONU remotely and start the configuration.

     By default, the user name is **root** and the password is **mduadmin**.
  2. Globally configure the band plan type.

     ```
     huawei(config)#xdsl vectoring bandplan-type 998ade us0-type type-a
     ```
  3. Configure the policy for activating a vectoring legacy CPE.

     ```
     huawei(config)#xdsl vectoring legacy-cpe activate-policy no-limit
     ```
  4. Configure the policy for controlling frequent online and offline on ports.

     ```
     huawei(config)#xdsl frequent-retrain-control 0/1/0 control-policy no-limit
     ```
  5. Enable global vectoring.

Copyright © Huawei Technologies Co., Ltd.

```
huawei(config)#xdsl vectoring enable
```

6. Save the data.

```
huawei(config)#save
```

- Configuration procedure for the MA5603T:

1. Log in to the ONU remotely and start the configuration.

   By default, the user name is **root** and the password is **admin**.

2. Globally configure the band plan type.

```
huawei(config)#xdsl vectoring bandplan-type 998ade us0-type type-a
```

3. Configure the vectoring profile as **huawei** and bind it to the VDSL2 port in the vectoring group.

```
huawei(config)#xdsl vectoring-profile add control enable enable name
huawei
huawei(config)#interface vdsl 0/1
huawei(config-if-vdsl-0/1)#vectoring-config all profile-name huawei
huawei(config-if-vdsl-0/1)#quit
```

4. Configure the policy for activating a vectoring legacy CPE.

```
huawei(config)#xdsl vectoring legacy-cpe activate-policy no-limit
```

5. Configure the policy for controlling frequent online and offline on ports.

```
huawei(config)#xdsl frequent-retrain-control 0/1/0 control-policy no-limit
```

6. Enable the global vectoring.

```
huawei(config)#xdsl vectoring enable
```

7. Save the data.

```
huawei(config)#save
```

----End

11.3.2.9 Configuring H.248 Voice Service (on the ONU)

This topic describes how to configure the voice service on the ONU based on the H.248 protocol to provide the high quality and low cost VoIP service for users.

Prerequisites

- The media gateway controller (MGC) interface data and the PSTN user data corresponding to the media gateway (MG) interface is configured on the MGC.
- Ensure that the **Status** of the voice board on the ONU is **Normal** by running the **display board 0** command.

Precautions

1. An ONU supports both the H.248 and SIP protocols; however, these two protocols are mutually exclusive. You can run the **display protocol support** command to query the currently supported voice protocol.
2. If the voice protocol needs to be switched, you need to delete the MG interface first and run the **protocol support** command to switch the protocol. After the configuration is complete, save the configuration and restart the system to make the configured protocol take effect.

Copyright © Huawei Technologies Co., Ltd.

CAUTION

This operation interrupts the ongoing services carried on the currently used MG interface. Hence, exercise caution when performing this operation.

Data plan

For details about the data plan, see **11.2.5 Principle of VoIP Service Data Plan**.

Item			Data
MG interface data **NOTE** The data configuration must be the same as the data configuration on the MGC.	Media and signaling parameters	Media and signaling upstream VLANs	200
		Media and signaling upstream port	0/0/1
		Media IP address and signaling IP address	10.10.10.10/24
		Default gateway IP address	10.10.10.1/24
	MG interface ID		0
	Signaling port ID		2944
	IP address of the primary MGC		200.200.200.200/24
	Port ID of the primary MGC		2944
	Coding		Text
	Transmission mode		UDP
	H248 version that MG starts to negotiate		1 (the negotiation starts from V1)
Voice user configuration data	Phone number		83110001-83110024
	Terminal identification		Terminal layering is not supported and the terminal identification ranges from 0 to 23.
	User priority		Cat2 for phone 1 Cat3 for phone 2 to phone 24 (default)
	User type		Common user (DEL user by default)
Common parameter	System parameter		Default value
	Overseas parameter		Default value
	PSTN port attribute		Polarity-reversal

Copyright © Huawei Technologies Co., Ltd.

Item		Data
	Ringing current attribute	Default value

Procedure

Step 1 Log in to and configure the ONU.

You can remote log in to the ONU from the OLT to perform the configuration. The user name is **root** and the password is **mduadmin**.

Step 2 Configure the upstream VLAN interface.

Specify the upstream VLAN interface for the media stream and the signaling flows and configure the IP addresses of the Layer 3 interface. These IP addresses are the sources of the IP address pools for the media stream and the signaling flows.

1. Create an upstream VLAN.

   The VLAN ID is 200 and the VLAN is a smart VLAN.

   ```
   huawei(config)#vlan 200 smart
   ```

2. Add the upstream port to the created upstream VLAN.

   Add upstream port 0/0/1 to VLAN 2000.

   ```
   huawei(config)#port vlan 200 0/0 1
   ```

3. Configure the IP address of the Layer 3 interface.

   Enter the VLAN interface mode and configure the lP address of the Layer 3 interface to 10.10.10.10

   ```
   huawei(config)#interface vlanif 200
   huawei(config-if-vlanif200)#ip address 10.10.10.10 24
   huawei(config-if-vlanif200)#quit
   ```

Step 3 Configure the media and signaling IP address pools.

Configure both the media IP address and signaling IP address to 10.10.10.10 and the MG IP address to 10.10.10.1.

```
huawei(config)#voip
huawei(config-voip)#ip address media 10.10.10.10 10.10.10.1
huawei(config-voip)#ip address signaling 10.10.10.10
huawei(config-voip)#quit
```

NOTE

- You can configure the attributes of the MG interface only when the media IP address and the signaling IP address exist in the media and signaling IP address pools.
- The media IP address can be different from the signaling IP address. Plan the data according to actual networking.

Step 4 Configure static routes.

Because the IP address of the VLAN interface and the IP address (200.200.200.200/24) of the MGC are in different network segments, you need to configure a route for the network segment from gateway 10.10.10.1 to 200.200.200.0.

```
huawei(config)#ip route-static 200.200.200.0 24 10.10.10.1
```

Step 5 Add an MG interface.

Copyright © Huawei Technologies Co., Ltd.

Add an MG interface to communicate with the MGC, which ensures that the MGC can control the call connection through the MG interface. Add MG interface 0 according to the data plan.

```
huawei(config)#interface h248 0
  Are you sure to add MG interface?(y/n)[n]:y
```

Step 6 Configure the attributes of the MG interface.

Pay attention to the following when configuring the attributes of the MG interface according to the data plan:

- The MG interface is registered by the IP address (default mode) or domain name, which must be the same as that on the MGC.
- The negotiated H.248 protocol version is V1, V2 or V3 (default value). The interface may fail to be registered because some softswitches do not support V3.

```
huawei(config-if-h248-0)#if-h248 attribute mgip 10.10.10.10 mgport
 2944 code text transfer udp primary-mgc-ip1 200.200.200.200 primary-mgc-port
 2944 mg-media-ip1 10.10.10.10 start-negotiate-version 1
```

Step 7 Reset the MG interface.

```
huawei(config-if-h248-0)#reset coldstart
  Are you sure to reset MG interface?(y/n)[n]:y
huawei(config-if-h248-0)#quit
```

NOTE

- You must cold reset the MG interface after configuring. Otherwise, the MG interface does not take effect.
- The MG interface can be cold reset only after parameters mgip, mgport, primary-mgc-ip1 (or mgc-domain-name1), mgcport_1, code, transfer, and mg-media-ip are correctly configured.

Step 8 Configure the PSTN user data.

Configure phone numbers of users 0/3/0-0/3/23 to 83110001-83110024 in batches and terminal identification to 0.

- Phone numbers are used for only internal emergency standalone, that is, internal extensions call each other. Actual phone numbers are assigned by the MGC.
- If the user of the MG interface is configured to support terminal layering, you need not configure the terminal identification because the system automatically allocates it. If the user of the MG interface does not support terminal layering, the terminal identification is mandatory. The terminal identification must be unique on one MG interface.

```
huawei(config)#esl user
huawei(config-esl-user)#mgpstnuser batadd 0/3/0 0/3/23 0 terminalid 0 telno
83110001
```

Step 9 Configure the call priority of a PSTN user.

```
huawei(config-esl-user)#mgpstnuser modify 0/3/0 priority cat2
huawei(config-esl-user)#quit
```

Step 10 Configure all the PSTN ports to support polarity reversal.

Configure the physical attributes of the PSTN port to which the users belong to support polarity reversal so that the user supports polarity reversal accounting.

```
huawei(config)#pstnport
huawei(config-pstnport)#pstnport attribute batset 0/3/0 0/3/23 reverse-pole-pulse
enable
huawei(config-pstnport)#quit
```

Step 11 Save the data.

Copyright © Huawei Technologies Co., Ltd.

```
huawei(config)#save
```

----End

11.3.2.10 Configuring SIP Voice Service (on the ONU)

This topic describes how to configure voice services based on the Session Initiation Protocol (SIP) on an optical network unit (ONU). The voice over IP (VoIP) services have high quality, but require low cost.

Prerequisites

- The IP Multimedia Subsystem (IMS) interface data and public switched telephone network (PSTN) user data corresponding to the SIP interface is configured on the IMS.
- **Status** of the voice board on the ONU is normal. (To verify board status, run the **display board 0** command.)

Precautions

1. An ONU supports both the H.248 and SIP protocols; however, these two protocols are mutually exclusive. You can run the **display protocol support** command to query the currently supported voice protocol.
2. If the voice protocol needs to be switched, you need to delete the MG interface first and run the **protocol support** command to switch the protocol. After the configuration is complete, save the configuration and restart the system to make the configured protocol take effect.

CAUTION

This operation interrupts the ongoing services carried on the currently used MG interface. Hence, exercise caution when performing this operation.

Data Plan

For configuration rules and description of configuration items, see **11.2.5 Principle of VoIP Service Data Plan**.

Item			Data
SIP interface data **NOTE** (It must be the same as that on the IMS core network device.)	Media and signaling parameters	Media and signaling upstream VLAN	200
		Media and signaling upstream port	0/0/1
		Media IP address and signaling IP address	10.10.10.10/24

Copyright © Huawei Technologies Co., Ltd.

Item			Data
		Default gateway IP address	10.10.10.1/24
	SIP interface ID		0
	Signaling port ID		5060
	IP address of the main IMS equipment		200.200.200.200/24
	Port ID of the main IMS equipment		5060
	Coding scheme		Text
	Transmission mode		UDP
	Home domain name (SIP)		huawei
	Profile index (SIP)		1
Voice user configuration data	Phone number		83110001-83110024
	User priority		Phone 1 indicates Cat2. Phone 2 to phone 24 indicate Cat3 (default value).
	User type		Common user (the DEL user by default)
Common Parameter	System parameter		Default value
	Overseas parameter		Default value
	PSTN port attribute		Polarity-Reversing Pulse
	Ringing current attribute		Default value

Procedure

Step 1 Log in to and configure the ONU.

You can remote log in to the ONU from the OLT to perform the configuration. The user name is **root** and the password is **mduadmin**.

Step 2 Configure the upstream VLAN interface.

Specify the upstream VLAN interface for the media stream and the signaling flows and configure the IP addresses of the Layer 3 interface. These IP addresses are the sources of the IP address pools for the media stream and the signaling flows.

1. Create an upstream VLAN.

   The VLAN ID is 200 and the VLAN is a smart VLAN.

   ```
   huawei(config)#vlan 200 smart
   ```


Copyright © Huawei Technologies Co., Ltd.

2. Add the upstream port to the created upstream VLAN.

   Add upstream port 0/0/1 to VLAN 2000.

   ```
   huawei(config)#port vlan 200 0/0 1
   ```

3. Configure the IP address of the Layer 3 interface.

   Enter the VLAN interface mode and configure the lP address of the Layer 3 interface to 10.10.10.10

   ```
   huawei(config)#interface vlanif 200
   huawei(config-if-vlanif200)#ip address 10.10.10.10 24
   huawei(config-if-vlanif200)#quit
   ```

Step 3 Configure the media and signaling IP address pools.

Set the media IP address and signaling IP address to 10.10.10.10, and the media gateway to 10.10.10.1.

```
huawei(config)#voip
huawei(config-voip)#ip address media 10.10.10.10 10.10.10.1
huawei(config-voip)#ip address signaling 10.10.10.10
huawei(config-voip)#quit
```

NOTE

- Attributes of the MG interface can be configured only when the media IP address and the signaling IP address exist in the media and signaling IP address pools.
- The Media IP address and signaling IP address can be different. Data planning should be based on networking requirements.

Step 4 Configure static routes.

Because the IP address of the VLAN interface and that of the IMS (200.200.200.200/24) are in different network segments, the configured routes must be from gateway 10.10.10.1 to the network segment 200.200.200.0.

```
huawei(config)#ip route-static 200.200.200.0 24 10.10.10.1
```

Step 5 Add an SIP interface.

The SIP interface is used for IMS communication.

```
huawei(config)#interface sip 0
  Are you sure to add the SIP interface?(y/n)[n]:y
```

Step 6 Configure the basic attributes of the SIP interface.

```
huawei(config-if-sip-0)#if-sip attribute basic media-ip 10.10.10.10 signal-ip
 10.10.10.10 signal-port 5060 transfer udp primary-proxy-ip1 200.200.200.200
 primary-proxy-port 5060 home-domain huawei sipprofile-index 1
```

Step 7 (Optional) Configure the optional attributes of the SIP interface.

Run the **if-sip attribute optional** command to configure the optional attributes, including the domain name, description, register server uniform resource identifier (URI), phone context, and conference factory URI of the SIP interface.

Step 8 Reset the SIP interface.

```
huawei(config-if-sip-0)#reset
  Are you sure to reset the SIP interface?(y/n)[n]:y
huawei(config-if-sip-0)#quit
```

Step 9 Configure the SIP PSTN user data.

Configure in batches the phone numbers of users 0/3/0-0/3/23 to 83110001-83110024.

Copyright © Huawei Technologies Co., Ltd.

NOTE

- To configure the data of a single SIP PSTN user, run the **sippstnuser add** command.
- To configure the data of multiple SIP PSTN users in batches, run the **sippstnuser batadd** command.

```
huawei(config)#esl user
huawei(config-esl-user)#sippstnuser batadd 0/3/0 0/3/23 0 telno 83110001
```

Step 10 Configure call priorities for SIP PSTN users.

```
huawei(config-esl-user)#sippstnuser attribute set 0/3/0 priority cat2
huawei(config-esl-user)#quit
```

Step 11 Configure all the PSTN ports to support polarity reversal.

Configure the physical attributes of the PSTN port to which the users belong to support polarity reversal so that the user supports polarity reversal accounting.

```
huawei(config)#pstnport
huawei(config-pstnport)#pstnport attribute batset 0/3/0 0/3/23 reverse-pole-pulse enable
huawei(config-pstnport)#quit
```

Step 12 Save the data.

```
huawei(config)#save
```

----End

11.3.2.11 Configuring Link Aggregation, Congestion Control, and Security Policy

The global configuration of upstream link aggregation and queue scheduling based on priorities ensures service reliability. The global configuration of security policies ensures service security.

Context

Link aggregation provides a higher bandwidth and uplink reliability for optical line terminals (OLTs) by aggregating multiple uplink Ethernet ports to one link aggregation group (LAG). Link aggregation is recommended.

Congestion control places the packets to be sent from a port into multiple queues that are marked with different priorities. Then, the packets are sent based on queue priorities. Congestion control is recommended.

Security policies ensure system, user, and service security.

NOTE

Enable a service security function based on the service type. For details, see **11.2.7 Principle of Security Data Plan**.

Procedure

- Configure link aggregation.

  The following configurations are used as an example to configure link aggregation:

  - Uplink ports 0/19/0 and 0/19/1 are added to a LAG.
  - The two ports send packets upstream based on the packets' source MAC addresses.
  - The LAG works in Link Aggregation Control Protocol (LACP) static aggregation mode.

  ```
  huawei(config)#link-aggregation 0/19 0-1 ingress workmode lacp-static
  ```


Copyright © Huawei Technologies Co., Ltd.

- Configure queue scheduling.

  According to quality of service (QoS) planning principles, all packets are scheduled in strict priority (SP) mode and mapped to queues according to the packets' priorities. For details about QoS planning principles, see **11.2.2 Principle of QoS Data Plan**.

  ```
  huawei(config)#queue-scheduler strict-priority
  huawei(config)#cos-queue-map cos0 0 cos4 4 cos5 5 cos6 6
  ```

- Configure system security.
  - Enable deny of service (DoS) anti-attack on both the OLT and optical network units (ONUs).
    1. Run the **security anti-dos enable** command to globally enable DoS anti-attack.
    2. Run the **security anti-dos control-packet policy** command to configure a protocol packet processing policy that will be used when a DoS attack occurs.
    3. Run the **security anti-dos control-packet rate** command to configure the threshold for the rate of sending protocol packets to the CPU.
  - Enable IP address anti-attack on both the OLT and ONUs.

    Run the **security anti-ipattack enable** command to enable IP address anti-attack.
- Configure user security.
  - Enable MAC address anti-flapping on both the OLT and ONUs.

    Run the **security anti-macduplicate enable** command to enable MAC address anti-flapping.
  - Enable MAC address anti-spoofing on both the OLT and ONUs.
    1. In global config mode, run the **security anti-macspoofing enable** command to globally enable MAC address anti-spoofing.
    2. Enable MAC address anti-spoofing at VLAN level in global config mode or service profile mode:
       a. In global config mode, run the **security anti-macspoofing vlan** command to enable MAC address anti-spoofing.
       b. Perform the following operations to enable MAC address anti-spoofing in service profile mode:
          a. In global config mode, run the **vlan service-profile** command to create a VLAN service profile.
          b. Run the **security anti-macspoofing enable** command to enable MAC address anti-spoofing at VLAN level.
          c. Run the **commit** command to make the profile configuration take effect.
          d. Run the **quit** command to quit the VLAN service profile mode.
          e. Run the **vlan bind service-profile** command to bind the created VLAN service profile to a VLAN.
    3. (Optional) Run the **security anti-macspoofing max-mac-count** command to set the maximum number of MAC addresses that can be bound to a service flow.
    4. (Optional) Run the **security anti-macspoofing exclude** command to configure the types of packets for which MAC address anti-spoofing does not take effect, such as Internet Group Management Protocol (IGMP) packets.
  - Enable IP address anti-spoofing on ONUs.

Copyright © Huawei Technologies Co., Ltd.

IP address anti-spoofing can be enabled or disabled at three levels: global, VLAN, and service port levels. This function takes effect only after it is enabled at the three levels. Among the three levels, IP address anti-spoofing is disabled only at the global level by default.

1. In global config mode, run the **security anti-ipspoofing enable** command to enable IP address anti-spoofing at the global level.
2. In VLAN service profile mode, run the **security anti-ipspoofing enable** command to enable IP address anti-spoofing at the VLAN level.
3. Run the **security anti-ipspoofing service-port** *serviceport-id* **enable** command to enable IP address anti-spoofing at the service port level.

- Configure service security.
  - Enable Dynamic Host Configuration Protocol (DHCP) Option 82 on both the OLT and ONUs. This configuration is recommended for the DHCP-based Internet access service.
    1. Enable DHCP Option 82 on both the OLT and ONUs.

       DHCP Option 82 can be enabled or disabled at four levels: global, port, VLAN, and service port levels. This function takes effect only after it is enabled at the four levels. Among the four levels, DHCP Option 82 is disabled only at the global level by default.
       - The global level: In global config mode, run the **dhcp option82** command to enable DHCP Option 82 at the global level.

         When you run this command, select the **enable**, **forward**, or **rebuild** parameter based on site requirements. The three parameters can all enable DHCP Option 82 but provide different packet processing policies on the OLT. For details, see the **dhcp option82** command.
       - The port level: In global config mode, run the **dhcp option82 port** or **dhcp option82 board** command to enable DHCP Option 82 at the port level.
       - The VLAN level:
         a. In global config mode, run the **vlan service-profile** command to create a VLAN service profile.
         b. Run the **dhcp option82 enable** command to enable DHCP Option 82 at the VLAN level.
         c. Run the **commit** command to make the profile configuration take effect.
         d. Run the **quit** command to quit the VLAN service profile mode.
         e. Run the **vlan bind service-profile** command to bind the created VLAN service profile to a VLAN.
       - The service port level: In global config mode, run the **dhcp option82 service-port** command to enable DHCP Option 82 at the service port level.
    2. On the OLT, run the **dhcp-option82 permit-forwarding service-port** command with the **enable** parameter selected, to allow ONU DHCP packets to carry Option 82 information.
  - Enable Policy Information Transfer Protocol (PITP) on both the OLT and ONUs. This configuration is recommended for the PPPoE-based Internet access service.
    1. Enable PITP on both the OLT and ONUs.

Copyright © Huawei Technologies Co., Ltd.

PITP can be enabled or disabled at four levels: global, port, VLAN, and service port levels. This function takes effect only after it is enabled at the four levels. Among the four levels, PITP is disabled only at the global level by default.

- The global level: In global config mode, run the **pitp enable pmode**, **pitp forward pmode**, or **pitp rebuild pmode** command to enable PITP at the global level.

  In the preceding commands, the **enable**, **forward**, and **rebuild** parameters can all enable PITP but provide different packet processing policies on the OLT. Select one of them based on site requirements. For details, see the **pitp** command.
- The port level: In global config mode, run the **pitp port** or **pitp board** command to enable PITP at the port level.
- The VLAN level:
  a. In global config mode, run the **vlan service-profile** command to create a VLAN service profile.
  b. Run the **pitp enable** command to enable PITP at the VLAN level.
  c. Run the **commit** command to make the profile configuration take effect.
  d. Run the **quit** command to quit the VLAN service profile mode.
  e. Run the **vlan bind service-profile** command to bind the created VLAN service profile to a VLAN.
- The service port level: In global config mode, run the **pitp service-port** command to enable PITP at the service port level.

2. On the OLT, run the **pitp permit-forwarding service-port** command with the **enable** parameter selected, to allow ONU PPPoE packets to carry a vendor tag.

----End

11.3.2.12 Verifying Services

In the Fiber-to-the-building (FTTB) scenario, optical network units (ONUs) are installed in buildings that are far from the central equipment room. ONUs support methods of remote service verification such as Point-to-Point Protocol over Ethernet (PPPoE) dialup emulation and call emulation. Remote site verification eliminates the need to go to site for a second time.

Prerequisites

ONUs are properly connected to upper-layer devices. The broadband remote access server (BRAS) and media gateway controller (MGC)/IP Multimedia Subsystem (IMS) have been configured.

Copyright © Huawei Technologies Co., Ltd.

Background Information

Remote Service Verification Method	Function	Remarks
PPPoE emulation dialup	By emulating PPPoE terminal software, an ONU dials up and interacts with the BRAS, to verify the connectivity between the ONT and BRAS.	PPPoE dialup emulation requires a service flow that does not belong to a QinQ VLAN. The user name, password, and authentication mode must be configured on the BRAS before the PPPoE dialup emulation starts. An ONU supports a maximum of one PPPoE dialup emulation.
Call emulation	An ONU emulates a call to check whether the voice service configurations are correct. The call emulation function can also be used to locate faults when a voice service is faulty.	● An ONU can emulate a caller or callee in an emulation test. A functional phone is required in the central office where the acceptance personnel is. ● An ONU can emulate the caller and callee simultaneously in an emulation test. No phone is required in the test. ● An ONU supports a maximum of one call emulation.

Data Plan

Item	Data	Remarks
PPPoE dialup emulation parameter	Service flow ID: 101 Emulation timer: 10s	The user name, password, and authentication mode required by the emulation test must be consistent with those configured on the BRAS.
Call emulation parameter	Caller port: 0/3/0 Called port: 0/3/23 Called number: 83110024	When an ONU simultaneously emulates the caller and the callee in an emulation test, retain the parameter settings as default. To query default values, run the **display pots emulational configuration** command.

Copyright © Huawei Technologies Co., Ltd.

Procedure

- Verify the Internet access service using PPPoE dialup emulation.
  1. Start an emulation test by running the **simulate dhcp start** command.

```
huawei(config)#pppoe simulate start
  Command:
          pppoe simulate start
 Service-port(index<0-999>):101
 User Name(length<1,65>):user0
 User Password(length<0,16>):*******
 Authentication Mode:
 1. Chap  2. Pap [default 1]:1
 Overtime Time(5-60s)[default 5]:10
```

  2. Query the emulation test information by running the **display pppoe simulate info** command.

```
huawei(config)#display pppoe simulate info
  PPPoE simulate information is:
  ------------------------------------------------------------------
  Service-port:  101
  User name:     user0
  Current phase: -                     //*Emulation phase
  Result:        Success               //*Emulation result
  Start time:    2011-11-16 15:41:29+08:00
  End time:      2011-11-16 15:41:34+08:00
  Session ID:    591
  User IP:       192.168.50.2
  Gateway IP:    192.168.50.254
  ------------------------------------------------------------------
```

  3. Terminate the emulation test by running the **simulate dhcp start** command.

```
huawei(config)#pppoe simulate stop
```

- Verify the voice service using call emulation.
  1. Start an emulation test by running the **ont emulational call** command.

```
huawei(config)#test
huawei(config-test)#pots emulational-call caller-port 0/3/0 callee-port
0/3/23 callee-telno 83110024
```

  2. The ONU outputs the call emulation result after the test is complete.

     The ONU outputs the call emulation result and failure of the cause if the emulation test fails.

```
huawei(config-test)#
  Caller port               :  0/3/0
  Callee port               :  0/3/23
  Test result               :  Test Succeed
```

----End

11.3.3 FTTB/FTTC+HGW Networking (Voice Service Provided by ONU)

The home gateway (HGW) provides Internet access and Internet Protocol television (IPTV) services. The services are sent upstream to the optical network unit (ONU) over a local area network (LAN) or x digital subscriber line (xDSL). The Integrated Access Device (IAD) in the ONU provides voice services.

11.3.3.1 Service Requirements and Application Scenario

Copyright © Huawei Technologies Co., Ltd.

Service Requirements

A gigabit-capable passive optical network (GPON) should be capable of delivering triple play service over Category 5 cables or twisted pairs. Service requirements are described as follows:

- Sharing of Internet access among multiple computers in the household
- Access of multiple phones in the household
- Internet Protocol (IPTV) services (program preview or watch) enabled by set-top boxes (STB)
- Independent provisioning of Internet access, voice, and IPTV services
- Ensured service security:
  - Internet access services protected against unauthorized access, hijacking or unauthorized borrowing of user accounts, MAC/IP spoofing, and malicious attack
  - Voice and IPTV services protected against MAC/IP spoofing, malicious attack, and traffic flooding attack
- Easy fault location and service maintenance

Application Scenario

As shown in **Figure 11-7**, a GPON optical line terminal (OLT) is deployed at the central office (CO), where services are converged into the metropolitan area network. An optical network unit (ONU) is deployed in the building corridor or the curb (fiber distribution terminal). Service access ports are provided by the local area network (LAN) or the home gateway (HGW) of an x digital subscriber line (xDSL) upstream.

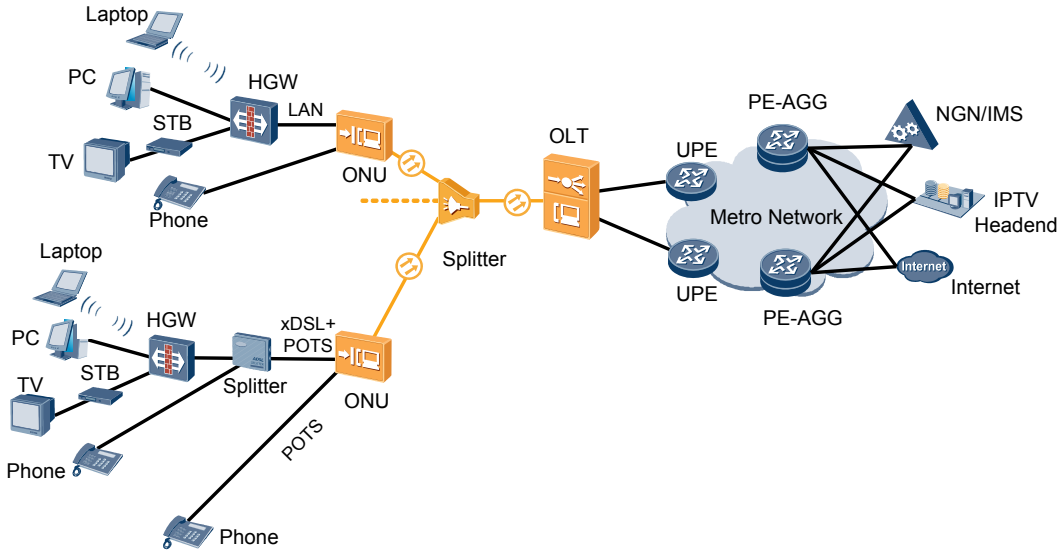
- An HGW sends services upstream to an ONU through ETH or xDSL ports, and provides Internet services for downstream subscribers through fast Ethernet (FE) ports or WiFi, and IPTV services through FE ports.
- The HGW has Layer 3 functions (such as PPPoE dialup and NAT), which enable multiple PCs of a family to access the Internet at the same time (NAT is short for network address translation).
- Set-top boxes (STB) are connected to HGWs to provide IPTV services (program preview and watch).
- The integrated access device (IAD) in an ONU provides at least one plain old telephone service (POTS) interface, which allows for access of multiple phones in the household.

The ONUs used in this application scenario include MA5822, MA5616, MA5622A, MA5603T, MA5612.

- LAN ports are available on MA5616, MA5822, MA5612.
- xDSL ports are available on MA5616, MA5622A, MA5603T.

Copyright © Huawei Technologies Co., Ltd.

Figure 11-7 GPON FTTB+HGW networking Diagram (voice, Internet access and IPTV services)

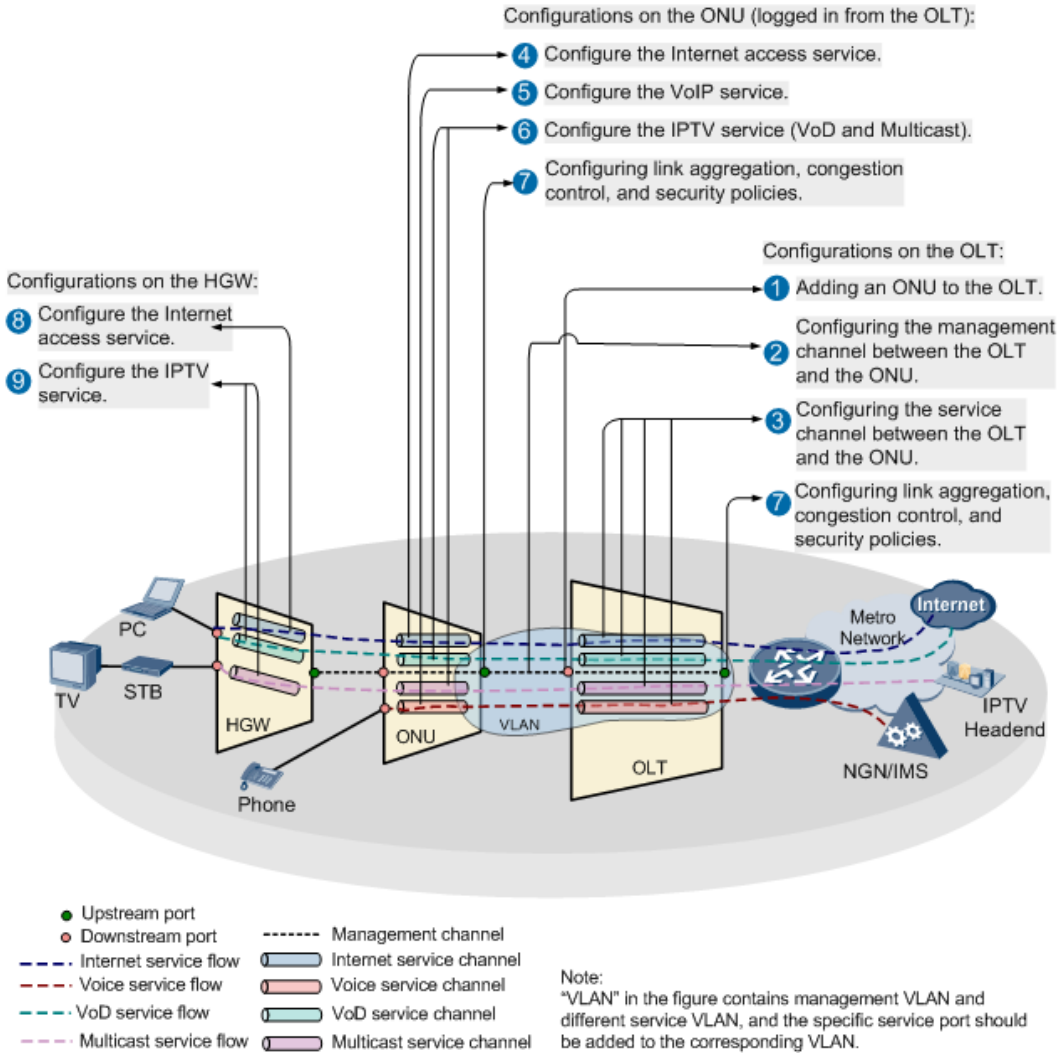


11.3.3.2 Configuration Procedure

Figure 11-8 shows the configuration roadmap diagram in the FTTB+HGW networking scenarios (ONU providing the VoIP service).

Copyright © Huawei Technologies Co., Ltd.

Figure 11-8 Configuration Roadmap Diagram in the FTTB+HGW Networking Scenarios (ONU Providing the VoIP Service)



The following table lists the configuration procedure..

Item	Procedure	Remarks
OLT	**Add an ONU on the OLT.**	Services can be configured for an ONU only after the ONU is successfully added to an OLT.
	Configure the management channel between the OLT and the ONU.	After the inband management channel between the OLT and the ONU is configured and available, you can log in to the ONU from the OLT to configure the ONU.

Copyright © Huawei Technologies Co., Ltd.

Item	Procedure		Remarks
	Configure the management channel between the OLT and the ONU.	● Configure the Internet access service channel. ● Configure the VoIP service channel. ● Configure the VoD service channel ● Configure the multicast service channel.	In the FTTB+HGW networking (ONU provides the voice service), the ONU provides the Internet and voice services and the HGW provides the IPTV service. Therefore, you need to create specific service channels for various services on the OLT.
ONU	Configure the Internet access service.	**Configure the LAN Internet access service on the ONU.**	**NOTE** Different ONUs have different ports, including LAN, ADSL2+, VDSL2, and VDSL2 vectoring ports, for the Internet access. Select an appropriate configuration method according to the port type.
		Configure the ADLS2+ Internet access service on the ONU.	
		Configure the VDSL2 Internet access service on the ONU.	
		(Optional) Configure vectoring on the ONU	
	Configure the VoIP service.	**Configure the H.248 -based VoIP service on the ONU.**	**NOTE** The H.248 and SIP protocols are mutually exclusive for the VoIP service. Only one of them is configured at a time.
		Configure the SIP-based VoIP service on the ONU.	

Copyright © Huawei Technologies Co., Ltd.

Item	Procedure		Remarks
	Configure the IPTV service.	● Configure the VoD service. ● Configure the multicast service.	IPTV services include the VoD and multicast services that are different in configuration procedures and need to be configured separately.
OLT ONU	**Configure the link aggregation, congestion control, and security policy.**		The global configuration of upstream link aggregation and queue scheduling based on priorities ensures service reliability. The global configuration of security policies ensures service security.
HGW	**Configure the Internet access service on the HGW.**		HGWs have different models and appearances but their configuration procedures are similar. This topic uses the HG239 that uses LAN for upstream transmission and the HG527 uses ADSL2+ for upstream transmission as examples. **NOTE** Vectoring is supported by the HG612 and HG622 only.
	Configure the IPTV service on the HGW.		-
ONU	**Verify the services.**		The ONU provides remote verification methods including PPPoE dialup emulation, call emulation and multicast emulation for the commissioning and configuration engineers to verify services remotely after service configuration, avoiding a second on-site operation.

11.3.3.3 Adding an ONU to an OLT

Services can be configured for an ONU only after the ONU is successfully added to an OLT.

Context

- When an ONU is added, corresponding profiles need to be bound to the ONU, including the dynamic bandwidth allocation (DBA) profile, line profile, and alarm profile. For details about functions and configuration methods for these profiles, see **Table 11-17**.

Copyright © Huawei Technologies Co., Ltd.

Table 11-17 Introduction to ONU profiles

Profile Type	Function	Command
DBA profile	A DBA profile describes GPON traffic parameters. A T-CONT is bound to a DBA profile for dynamic bandwidth allocation, improving upstream bandwidth utilization.	Query a DBA profile. **display dba-profile** Add a DBA profile. **dba-profile add**
Line profile	A line profile describes binding between the T-CONT and the DBA profile, the QoS mode of the service flow, and mapping between the GEM port and the ONU-side service.	Query a line profile. **display ont-lineprofile** Add a line profile. **ont-lineprofile add**
Alarm profile	An alarm profile contains a series of alarm threshold parameters that are used for performance measurement and monitoring of the activated ONT lines.	Query an alarm profile. **display gpon alarm-profile** Add an alarm profile. **gpon alarm-profile add**

- An ONU can be added in two modes. Select either mode as required.

Mode	Usage Scenario	Command
Add an ONU offline.	The ONU password or serial number (SN) is obtained.	Run the **ont add** command to add an ONU.
Online confirm an ONU.	Both the ONU password and SN are not obtained.	In the GPON mode, run the **port ont-auto-find** command to enable the ONU auto-discovery function of a GPON port and then run the **ont confirm** command to add an ONU.

Data plan

Table 11-18 Data plan

Item	Data
DBA profile	Profile name: fttb_dba Profile type: type3 Assured bandwidth: 8 Mbit/s Maximum bandwidth: 20 Mbit/s

Copyright © Huawei Technologies Co., Ltd.

Item	Data
Line profile	Profile name: fttb(c) Profile ID: 10 T-CONT ID: 4 GEM port ID for management service: 11 GEM port ID for Internet access service: 12 GEM port ID for VoIP service: 13
Network topology data	PON port: 0/2/1 ONT ID: 1

Procedure

Step 1 Configure GPON ONU profiles.

1. Configure a DBA profile.

   ```
   huawei(config)#dba-profile add profile-name fttb_dba type3 assure 8192 max 20480
   ```

2. Configure an ONU line profile.

   a. Add GPON ONU line profile 10 fttb(c).

   ```
   huawei(config)#ont-lineprofile gpon profile-id 10 profile-name fttb(c)
   ```

   NOTE

   The ID of the line profile to be created must not exist in the system and the line profile must be created according to the data plan. In this example, line profile 10 is used.

   b. In the line profile mode, bind T-CONT 4 to DBA profile fttb_dba.

   ```
   huawei(config-gpon-lineprofile-10)#tcont 4 dba-profile-name fttb_dba
   ```

   c. In the line profile mode, bind the GEM port to the T-CONT.

   - Add GEM port 11 to carry management service flows.
   - Add GEM port 12 to carry Internet access service flows.
   - Add GEM port 13 to carry VoIP service flows.

   Bind GEM ports 11, 12, and 13 to T-CONT 4. In configuring, QoS policies for various service flows also need to be configured. For details about QoS data plan, see **11.2.2 Principle of QoS Data Plan**.

   ```
   huawei(config-gpon-lineprofile-10)#gem add 11 eth tcont 4 cascade on
   huawei(config-gpon-lineprofile-10)#gem add 12 eth tcont 4 cascade on
   huawei(config-gpon-lineprofile-10)#gem add 13 eth tcont 4 cascade on
   ```

   d. Configure mapping between the GEM port and the ONU-side service.

   Set the mode for mapping the GEM port to the ONU-side service to the VLAN mapping mode (default). Map management service flows (the CVLAN ID is 8) to GEM port 11, Internet access service flows (the CVLAN ID is 1001) to GEM port 12, and VoIP service flows (the CVLAN ID is 200) to GEM port 13.

   ```
   huawei(config-gpon-lineprofile-10)#gem mapping 11 0 vlan 8
   huawei(config-gpon-lineprofile-10)#gem mapping 12 1 vlan 1001
   huawei(config-gpon-lineprofile-10)#gem mapping 13 2 vlan 200
   ```


Copyright © Huawei Technologies Co., Ltd.

e. After the configuration is completed, run the **commit** command to make the configured parameters take effect.

```
huawei(config-gpon-lineprofile-10)#commit
huawei(config-gpon-lineprofile-10)#quit
```

3. (Optional) Add an alarm profile.
   - The ID of the default GPON alarm profile is 1. The thresholds for all the alarm parameters in the default alarm profile are 0, which indicates that no alarm is generated.
   - In this example, the default alarm profile is used and therefore the configuration of the alarm profile is not required.

Step 2 Add an ONU to an OLT.

Assume that the ID of GPON port 0/2/1 is 1, SN is 32303131B39FD641, management mode is SNMP, and the bound line profile is fttb(c). Connect the ONU to such a GPON port through the optical splitter.

There are two modes to add an ONT: add an ONT offline and confirm an automatically discovered ONU.

- Add an ONU offline.

```
huawei(config)#interface gpon 0/2
huawei(config-if-gpon-0/2)#ont add 1 ontid 1 sn-auth 32303131B39FD641
snmp ont-lineprofile-name fttb(c)
```

- Confirm an automatically discovered ONU.

```
huawei(config)#interface gpon 0/2
huawei(config-if-gpon-0/2)#port 1 ont-auto-find enable
huawei(config-if-gpon-0/2)#display ont autofind 1
huawei(config-if-gpon-0/2)#ont confirm 1 ontid 1 sn-auth 32303131B39FD641
snmp ont-lineprofile-name fttb(c)
```

1. (Optional) Bind the alarm profile to the ONU.

   By default, alarm profile 1 automatically bound to an ONU. A non-default alarm profile is bound manually only when the default one does not meet the requirement.

   In this example, default alarm profile 1 is used and therefore the configuration of the alarm profile is not required.

Step 3 Check the ONU status.

After an ONU is added, run the **display ont info** command to query the current status of the ONU. Ensure that **Config flag** of the ONU is **active**, **Run State** is **online**, and **Config state** is **normal**.

```
huawei(config-if-gpon-0/2)#display ont info 1 1
  ------------------------------------------------------------------------
  F/S/P                : 0/2/1
  ONT-ID               : 1
  Control flag         : active    //The ONU is activated.
  Run state            : online    //The ONU is online.
  Config state         : normal    //The ONU configurations are recovered
normally.
...//The rest of the response information is not provided here.
huawei(config-if-gpon-0/2)#quit
```

----End

Follow-up Procedure

When **Config state** is **failed**, **Run state** is **offline**, or **Match state** is **mismatch**:

Copyright © Huawei Technologies Co., Ltd.

- If **Control flag** is **deactive**, run the **ont active** command in GPON mode to activate the ONU.
- If **Run state** is **offline**, a physical line may be broken or the optical module may be damaged. Check the line and the optical module.
- If **Config state** is **failed**, the configured ONU capability exceeds the actual ONU capability. In this case, run the **display ont failed-configuration** command in the diagnose mode to check the failed configuration item and the failure cause. Then, rectify the fault accordingly.
- If the ONU does not match, that is, **Match state** is **mismatch**, the port types and number of ports undermatch the actual port types and number of ports supported by the ONU. In this case, run the **display ont capability** command to query the actual capability of the ONU, and then select one of the following modes to modify the ONU configuration:
  - Create a proper ONU profile according to the actual capability of the ONU, and then run the **ont modify** command to modify the configuration data of the ONU.
  - Modify the ONU profile according to the actual capability of the ONU and save the modification. Then, the ONU automatically recovers the configuration successfully.

11.3.3.4 Configuring the Management Channel Between the OLT and the ONU

After the inband management channel between the OLT and the ONU is configured and available, you can log in to the ONU from the OLT to configure the ONU.

Data plan

Item	Data	Remarks
Management VLAN and management IP address on the OLT side	Management VLAN ID: 8 Management VLAN type: smart VLAN Inband management IP address: 192.168.50.1/24	To configure the MDU from the OLT by remote logging in to the MDU, the management VLAN of the OLT and that of the MDU must be the same, and the management IP address of the OLT and that of the MDU must be in the same network segment.
Management VLAN and management IP address on the ONU side	Management VLAN ID: 8 Management VLAN type: smart VLAN Inband management IP address: 192.168.50.2/24	

Procedure

Step 1 Configure the inband management VLAN and IP address of the OLT.

Configure the inband management VLAN to 8, VLAN priority to 6, and the IP address to 192.168.50.1/24.

```
huawei(config)#vlan 8 smart
huawei(config)#port vlan 8 0/19 0
huawei(config)#vlan priority 8 6
huawei(config)#interface vlanif 8
```


Copyright © Huawei Technologies Co., Ltd.

```
huawei(config-if-vlanif8)#ip address 192.168.50.1 24
huawei(config-if-vlanif8)#quit
```

Step 2 Configure the inband management VLAN and IP address of the ONU.

Configure the static IP address of the ONU to 192.168.50.2/24, gateway to 192.168.50.254, and the management VLAN ID to 8 (the same as the management VLAN of the OLT).

```
huawei(config)#interface gpon 0/2
huawei(config-if-gpon-0/2)#ont ipconfig 1 1 static ip-address 192.168.50.2 mask
255.255.255.0 gateway
192.168.50.254 vlan 8
huawei(config-if-gpon-0/2)#quit
```

Step 3 Configure an inband management service port.

Configure the management service port ID to 1, management VLAN ID to 8, GEM port ID to 11, and user-side VLAN ID to 8. The OLT does not limit inband management service flows. Therefore, it is recommended that you use default traffic profile 6.

```
huawei(config)#service-port 1 vlan 8 gpon 0/2/1 ont 1 gemport 11 multi-service
user-vlan 8 rx-cttr 6 tx-cttr 6
```

Step 4 Confirm that the management channel between the OLT and the ONU is available.

- On the OLT, run the **ping *192.168.50.2*** command to check the connectivity between the OLT and the ONU. The ICMP ECHO-REPLY packet from the ONU should be received.
- On the OLT, you can remote log in to the ONU to perform the configuration.

----End

11.3.3.5 Configuring Service Channels Between an OLT and an ONU

This topic describes how to configure service channels between an optical line terminal (OLT) and an optical network unit (ONU) on a gigabit-capable passive optical network (GPON). After channels for involved service types are configured on an OLT to which an ONU is connected, packets of the service types from the ONU can be forwarded based on planned VLANs and policies at Layer 2.

Prerequisites

1. **11.3.1.3 Adding an ONU to an OLT** is performed.
2. **11.3.1.4 Configuring the Management Channel Between the OLT and the ONU** is performed.

Data Plan

The following table provides key information about the service channels between an OLT and an ONU.

Copyright © Huawei Technologies Co., Ltd.

Service Type	VLAN Plan	Remarks
Internet access service	S-VLAN ID: 100; S-VLAN attribute: stacking C-VLAN ID: 1000-1016	Plan the Internet access service in per user per service per VLAN (PUPSPV) mode and apply S-VLAN+C-VLAN to differentiate users. For details, see **11.2.3 Principle of Internet Access Service Data Plan**.
VoIP service	S-VLAN ID: 200 C-VLAN ID: 200	The voice over IP (VoIP) service is a carrier-operating, closed service and primarily adopts only S-VLAN tags, which are transparently transmitted by OLTs. For details, see **11.2.5 Principle of VoIP Service Data Plan**.
VoD service	S-VLAN ID: 300	Plan the video on demand (VoD) service in per user per VLAN (PUPV) mode if possible, as the VoD service requires only a few VLAN resources. The VoD service is a carrier-operating, closed service and primarily adopts only S-VLAN tags, which are transparently transmitted by OLTs. For details, see **11.2.6 Principle of IPTV Service Data Plan**.
Multicast service	Multicast VLAN ID: 1000 Multicast cascading port: 0/2/1 IGMP version: IGMPv3 IGMP mode: IGMP proxy Multicast IP address range: 224.1.1.10-224.1.1.100 IP address of the multicast server: 10.10.10.10/24	The multicast service is a carrier-operating, closed service and primarily adopts only S-VLAN tags. For details, see **11.2.6 Principle of IPTV Service Data Plan**.

NOTE

C-VLANs in the preceding table are defined for OLTs. That is, they are upstream VLANs or S-VLANs of ONUs.

Procedure

- Configure a channel for the Internet access service.
  1. Create an S-VLAN and add an upstream port to it.

Copyright © Huawei Technologies Co., Ltd.

Create S-VLAN 100 with the stacking attribute and add upstream port 0/19/0 to the S-VLAN.

```
huawei(config)#vlan 100 smart
huawei(config)#vlan attrib 100 stacking
huawei(config)#port vlan 100 0/19 0
```

2. Configure a traffic profile.

   The 802.1p priority of the Internet access service is 0, and rate limitation is not required. To check whether any existing traffic profile meets the requirements, run the **display traffic table ip** command. In this example, the query result shows that traffic profile 6 meets the requirements, so no traffic profile needs to be configured.

   ```
   huawei(config)#display traffic table ip from-index 0
   ```

3. Configure a service flow for receiving and transparently transmitting the Internet access service from the ONU side.

   Configure a service flow with the GEM port ID being 12 and user-side VLAN ID being 1001 (example value). The ONU is connected to GPON port 0/2/1, upstream and downstream traffic are rate-limited on the ONU but not on the OLT, and traffic profile 6 is referenced.

   ```
   huawei(config)#service-port vlan 100 gpon 0/2/1 ont 1 gemport 12 multi-
   service user-vlan 1001 tag-transform translate-and-add rx-cttr 6 tx-cttr 6
   ```

- Configure a channel for the VoIP service.

  1. Create an S-VLAN and add an upstream port to it.

     Create S-VLAN 200 with the common attribute and add upstream port 0/19/0 to the S-VLAN.

     ```
     huawei(config)#vlan 200 smart
     huawei(config)#port vlan 200 0/19 0
     ```

  2. Configure a traffic profile.

     The 802.1p priority of the VoIP service is 5, and rate limitation is not required. To check whether any existing traffic profile meets the requirements, run the **display traffic table ip** command. In this example, the query result shows that no traffic profile meets the requirements, so a traffic profile needs to be configured.

     Add traffic profile 9 and set *priority-policy* to **local-setting**. Then, traffic is scheduled based on the priority specified in the traffic profile.

     ```
     huawei(config)#traffic table ip index 9 cir off priority 5 priority-policy
     local-setting
     ```

  3. Configure a service flow for receiving and transparently transmitting the VoIP service from the ONU side.

     Configure a service flow with the GEM port ID being 13 and user-side VLAN ID being 200. The ONU is connected to GPON port 0/2/1, upstream and downstream traffic are rate-limited on the ONU but not on the OLT, and traffic profile 9 is referenced.

     ```
     huawei(config)#service-port vlan 200 gpon 0/2/1 ont 1 gemport 13 multi-
     service user-vlan 200 rx-cttr 9 tx-cttr 9
     ```

- Configure a channel for the VoD service.

  1. Create an S-VLAN and add an upstream port to it.

Copyright © Huawei Technologies Co., Ltd.

Create S-VLAN 300 with the common attribute and add upstream port 0/19/0 to the S-VLAN.

```
huawei(config)#vlan 300 smart
huawei(config)#port vlan 300 0/19 0
```

2. Configure a traffic profile.

   The 802.1p priority of the VoD service is 4, and rate limitation is not required. To check whether any existing traffic profile meets the requirements, run the **display traffic table ip** command. In this example, the query result shows that no traffic profile meets the requirements, so a traffic profile needs to be configured.

   Add traffic profile 10 and set *priority-policy* to **local-setting**. Then, traffic is scheduled based on the priority specified in the traffic profile.

   ```
   huawei(config)#traffic table ip index 10 cir off priority 4 priority-policy local-Setting
   ```

3. Configure a service flow for the VoD service.

   Configure a service flow with the GEM port ID being 14 and user-side VLAN ID being 300. The ONU is connected to GPON port 0/2/1, upstream and downstream traffic are rate-limited on the ONU but not on the OLT, and traffic profile 10 is referenced.

   ```
   huawei(config)#service-port vlan 300 gpon 0/2/1 ont 1 gemport 14 multi-service user-vlan 300 rx-cttr 10 tx-cttr 10
   ```

- Configure a channel for the multicast service.

  1. Create an S-VLAN and add an upstream port to it.

     Create S-VLAN 1000 with the common attribute and add upstream port 0/19/0 to the S-VLAN.

     ```
     huawei(config)#vlan 1000 smart
     huawei(config)#port vlan 1000 0/19 0
     ```

  2. Configure a service flow for the multicast service.

     Configure a service flow with the GEM port ID being 14 and user-side VLAN ID being 1000. ONT 1 is connected to GPON port 0/2/1, upstream and downstream traffic are rate-limited on the ONU but not on the OLT, and traffic profile 10 is referenced.

     ```
     huawei(config)#service-port vlan 1000 gpon 0/2/1 ont 1 gemport 14 multi-service user-vlan 1000 rx-cttr 10 tx-cttr 10
     ```

  3. Configure a multicast cascading port.

     Set GPON port 0/2/1 as a multicast cascading port, ONT ID to 1, and GEM port 14 to carry the multicast service.

     ```
     huawei(config)#btv
     huawei(config-btv)#igmp cascade-port 0/2/1 ontid 1 gemport-index 14
     ```

  4. Set the IGMP version.

     Set the IGMP version to IGMPv3.

     ```
     huawei(config)#multicast-vlan 1000
     huawei(config-mvlan1000)#igmp version v3
     ```

  5. Set the IGMP mode.

     Select the IGMP proxy mode.

Copyright © Huawei Technologies Co., Ltd.

```
huawei(config-mvlan1000)#igmp mode proxy
  Are you sure to change IGMP mode?(y/n)[n]:y
```

6. Configure an IGMP upstream port.

   Set the IGMP upstream port to port 0/19/0.

   ```
   huawei(config-mvlan1000)#igmp uplink-port 0/19/0
   ```

7. Configure a program library.

   Set the multicast IP address range to 224.1.1.10-224.1.1.100 and the IP address of the multicast server to 10.10.10.10.

   ```
   huawei(config-mvlan1000)#igmp program add batch ip 224.1.1.10 to-ip
   224.1.1.100 sourceip 10.10.10.10
   ```

----End

11.3.3.6 Configuring the Internet Access Service (LAN Access, on the ONU)

This topic describes how to configure the Internet access service for home gateway (HGW) users on an optical network unit (ONU) when HGWs are connected upstream to the ONU through local area networks (LANs).

Data Plan

The following table provides key information about the Internet access service (LAN access).

Item	Data	Remarks
Traffic profile	ID: 8 CIR: 4 Mbit/s VLAN priority: 0 Downstream priority policy: local-setting	-
User VLAN	Untagged	HGWs can send untagged packets or packets with user VLAN tags.
	User VLAN ID: 1, 2, 3...	

Procedure

Step 1 Log in to the ONU to perform the configuration.

You can remote log in to the ONU from the OLT to perform the configuration. User name: **root** (default). Password: **mduadmin** (default).

Step 2 Configure a traffic profile.

You can run the **display traffic table ip** command to query the traffic profiles existing in the system. If the traffic profiles existing in the system do not meet the requirements, you need to run the **traffic table ip** command to add a traffic profile.

Add traffic profile 8 and set the committed information rate (CIR) to 4 Mbit/s. The priority for upstream packets is 0, and downstream packets are scheduled based on the priority specified in the traffic profile.

Copyright © Huawei Technologies Co., Ltd.

```
huawei(config)#traffic table ip index 8 cir 4096 priority 0 priority-policy local-setting
```

Step 3 Create service VLANs.

Create service VLANs 1001-1016 in batches whose type is smart and attribute is common (the service VLAN IDs must be consistent with the user VLAN IDs of the OLT). Add the service VLANs to upstream port 0/0/1.

```
huawei(config)#vlan 1001-1016 smart
huawei(config)#port vlan 1001-1016 0/0 1
```

Step 4 Add a service port.

Configurations for untagged packets and packets with user VLAN tags are different.

- For untagged packets, the configuration is as follows (assuming that the VLAN ID is 1001):

```
   //Create service port 101, bind port 0/3/1 to it, set the user VLAN to untagged, and bind traffic profile 8 to the user VLAN./
huawei(config)#service-port 101 vlan 1001 eth 0/3/1 multi-service user-vlan untagged rx-cttr 8 tx-cttr 8
```

- For packets with user VLAN tags, the configuration is as follows (assuming that the user VLAN ID is 10 and the VLAN ID is 1001):

```
   //Create service port 101, bind port 0/3/1 to it, set the user VLAN ID to 10, and bind traffic profile 8 to the user VLAN./
huawei(config)#service-port 101 vlan 1001 eth 0/3/1 multi-service user-vlan 10 rx-cttr 8 tx-cttr 8
```

----End

11.3.3.7 Configuring the Internet Access Service (ADSL2+ Access, on the ONU)

This topic describes how to configure the Internet access service for home gateway (HGW) users on an optical network unit (ONU) when HGWs are connected upstream to the ONU in ADSL2 + mode.

Context

ADSL2+ ports working in normal mode (that is, RFC 2662 mode) need to bind an ADSL2+ line profile and an ADSL2+ alarm profile. For the functions and configurations of each profile, see **Table 11-19**.

Copyright © Huawei Technologies Co., Ltd.

Table 11-19 ADSL2+ profile

Profile Type	Function	Configuration
ADSL2+ line profile	An ADSL2+ line profile provides the following parameters: ● ADSL/ADSL2+ working mode ● Channel mode ● Upstream/Downstream line rate ● Upstream/Downstream interleave depth ● Noise margin When an ADSL2+ port is activated, the central office (CO) and the customer premises equipment (CPE) negotiate based on the parameters configured in the ADSL2+ line profile, to determine whether the ADSL2+ port can work in the normal state in these conditions.	The system has four default profiles (profile 1, profile 1022, profile 1023, and profile 1024) for activation of ADSL2+ ports in different conditions. ● Profile 1 is used for activation of common ADSL ports. ● Profile 1022 is used for fast activation of ADSL ports. ● Profile 1023 is used for long-reach activation of existing ADSL ports. ● Profile 1024 is used for activation of ports on ADSL2+ boards. Commands: ● To query: **display adsl line-profile** ● To add: **adsl line-profile add** or **adsl line-profile quickadd**
ADSL2+ alarm profile	Values to be configured in an ADSL2 + line alarm profile are thresholds within any 15 minutes. When the statistics of an item reach the threshold, the system informs the device of the event and sends alarms to the NMS.	Commands: ● To query: **display adsl alarm-profile** ● To add: **adsl alarm-profile add** or **adsl alarm-profile quickadd**

Data Plan

The following table provides key information about the Internet access service (ADSL2+ access).

Item	Data	Remarks
Traffic profile	ID: 8 CIR: 4 Mbit/s VLAN priority: 0 Downstream priority policy: local-setting	A traffic profile implements rate-limiting.
VPI/VCI of ADSL2+ users	VPI: 0 VCI: 35	Internet service providers (ISPs) provide VPI/VCI information.

Copyright © Huawei Technologies Co., Ltd.

Item	Data	Remarks
ADSL2+ line profile	ID: 1024 (default); key parameters: ● Working mode: full compatibility ● Channel working mode: interleaved ● Maximum upstream/ downstream rate (kbit/s): 24544/1024	A traffic profile or an ADSL2+ line profile can implement rate-limiting on ADSL2+ ports. This example uses a default traffic profile.
ADSL2+ alarm profile	ID: 1 (default)	The system does not check whether parameter thresholds are crossed and so does not report alarms.

Procedure

Step 1 Log in to the ONU to perform the configuration.

You can remote log in to the ONU from the OLT to perform the configuration. User name: **root** (default). Password: **mduadmin** (default).

Step 2 Configure a traffic profile.

You can run the **display traffic table ip** command to query the traffic profiles existing in the system. If the traffic profiles existing in the system do not meet the requirements, you need to run the **traffic table ip** command to add a traffic profile.

Add traffic profile 8 and set the committed information rate (CIR) to 4 Mbit/s. The priority for upstream packets is 0, and downstream packets are scheduled based on the priority specified in the traffic profile.

```
huawei(config)#traffic table ip index 8 cir 4096 priority 0 priority-policy local-setting
```

Step 3 Create service VLANs.

Create service VLANs 1001-1016 in batches whose type is smart and attribute is common (the service VLAN IDs must be consistent with the user VLAN IDs of the OLT). Add the service VLANs to upstream port 0/0/1.

```
huawei(config)#vlan 1001-1016 smart
huawei(config)#port vlan 1001-1016 0/0 1
```

Step 4 Add a service port.

Assume that the VPI/VCI of users is 0/35 and the VLAN ID is 1001. Add a service port as follows:

```
   //Create service port 101, bind port 0/2/0 to it, set VPI/VCI to 0/35, and bind traffic profile 8 to the user VLAN./
huawei(config)#service-port 101 vlan 1001 adsl 0/2/0 vpi 0 vci 35 multi-service user-vlan untagged rx-cttr 8 tx-cttr 8
```

Step 5 (Optional) Configure an ADSL2+ line profile.

- Configure an ADSL2+ line profile only when the default one does not meet requirements.

Copyright © Huawei Technologies Co., Ltd.

- This example uses the default ADSL2+ line profile (ID: 1024).

Step 6 (Optional) Configure an ADSL2+ alarm profile.

This example uses the default ADSL2+ alarm profile (ID: 1).

Step 7 Bind an ADSL2+ line profile and an ADSL2+ alarm profile, and activate the ADSL2+ port.

For example, bind ADSL2+ line profile 1024 and ADSL2+ alarm profile 1, and activate ADSL2+ port 0/2/0.

```
huawei(config)#interface adsl 0/2
huawei(config-if-adsl-0/2)#deactivate 0
huawei(config-if-adsl-0/2)#alarm-config 0 1
huawei(config-if-adsl-0/2)#activate 0 profile-index 1024
```

----End

11.3.3.8 Configuring the Internet Access Service (VDSL2 Access, on the ONU)

This topic describes how to configure the Internet access service for home gateway (HGW) users on an optical network unit (ONU) when HGWs are connected upstream to the ONU in VDSL2 mode.

Context

VDSL2 ports working in normal mode (that is, TR129 mode) need to bind the VDSL2 line template and VDSL2 alarm template. For the functions and configurations of each profile, see **Table 11-20**.

Table 11-20 VDSL2 template

Template Type	Function	Configuration
VDSL2 line template	A VDSL2 line template consists of a VDSL2 line profile and a VDSL2 channel profile. When a VDSL2 port is activated, the central office (CO) and the customer premises equipment (CPE) negotiate based on the parameters configured in the VDSL2 line template, to determine whether the VDSL2 port can work in the normal state in these conditions.	The system has one default VDSL2 line template (template 1), which is used for activation of common VDSL2 ports. ● To query: **display vdsl line-template** ● To add: **vdsl line-template add** or **vdsl line-template quickadd**
	A VDSL2 line profile provides the following parameters: line transmission mode, adaptation mode of upstream/downstream transmit rates, signal-to-noise ratio (SNR) margin, upstream power back-off (UPBO), and downstream power back-off (DPBO).	● To query: **display vdsl line-profile** ● To add: **vdsl line-profile add** or **vdsl line-profile quickadd**

Copyright © Huawei Technologies Co., Ltd.

Template Type	Function	Configuration
	A VDSL2 channel profile provides the following parameters: data channel mode, minimum impulse noise protection, interleaved delay parameters, rate parameters, retransmission at the physical layer, erasure decoding, and G.998.4 retransmission.	● To query: **display vdsl channel-template** ● To add: **vdsl channel-template add** or **vdsl channel-profile quickadd**
VDSL2 alarm template	A VDSL2 alarm template consists of a VDSL2 line alarm profile and a VDSL2 channel alarm profile. Values to be configured in a VDSL2 alarm template are thresholds within any 15 minutes. When the statistics of an item reach the threshold, the system informs the device of the event, and sends alarms to the NMS.	The system has one default VDSL2 alarm template (template 1). ● To query: **display vdsl alarm-template** ● To add: **vdsl alarm-template add** or **vdsl alarm-template quickadd**
	A VDSL2 line alarm profile provides the following parameters for COs and CPEs: ● Forward error check seconds (FECS) ● Errored seconds (ES) ● Severely errored seconds (SES) ● Loss of signal seconds (LOSS) ● Unavailable seconds (UAS) ● Low error-free throughput rate (LEFTR) defect seconds	● To query: **display vdsl alarm-profile** ● To add: **vdsl alarm-profile add** or **vdsl alarm-profile quickadd**
	A VDSL2 channel alarm profile provides the following parameters for COs and CPEs: ● Coding violations counts (CVC) ● Corrected blocks counts (CBC)	● To query: **display vdsl channel-alarm-profile** ● To add: **vdsl channel-alarm-profile add** or **vdsl channel-alarm-profile quickadd**

Data Plan

Table 11-21 provides key information about the Internet access service (VDSL2 access).

Copyright © Huawei Technologies Co., Ltd.

Table 11-21 Key information about the Internet access service (VDSL2 access)

Item	Data	Remarks
Traffic profile	ID: 8 CIR: 4 Mbit/s VLAN priority: 0 Downstream priority policy: local-setting	A traffic profile implements rate-limiting.
VDSL2 line mode	PTM	There are two VDSL line modes: ATM mode and PTM mode. ● ATM mode: ATM cells are transmitted in channels. This mode is compatible with the ADSL2+ mode. ● PTM mode: IP cells are transmitted in channels. This mode is incompatible with the ADSL2+ mode. This example assumes the PTM mode.
VDSL2 line template	Line profile ID: 1 (default)	A traffic profile or a VDSL2 line template can implement rate-limiting on VDSL2 ports. This example uses a default traffic profile.
	Channel profile ID: 1 (default)	
	Line template ID: 1 (default)	
VDSL2 alarm template	Line alarm profile ID: 1 (default)	The system does not check whether parameter thresholds are crossed and so does not report alarms.
	Channel alarm profile ID: 1 (default)	
	Alarm template ID: 1 (default)	

Procedure

Step 1 Log in to the ONU to perform the configuration.

You can remote log in to the ONU from the OLT to perform the configuration. User name: **root** (default). Password: **mduadmin** (default).

Step 2 Configure a traffic profile.

You can run the **display traffic table ip** command to query the traffic profiles existing in the system. If the traffic profiles existing in the system do not meet the requirements, you need to run the **traffic table ip** command to add a traffic profile.

Add traffic profile 8 and set the committed information rate (CIR) to 4 Mbit/s. The priority for upstream packets is 0, and downstream packets are scheduled based on the priority specified in the traffic profile.

Copyright © Huawei Technologies Co., Ltd.

```
huawei(config)#traffic table ip index 8 cir 4096 priority 0 priority-policy local-setting
```

Step 3 Create service VLANs.

Create service VLANs 1001-1016 in batches whose type is smart and attribute is common (the service VLAN IDs must be consistent with the user VLAN IDs of the OLT). Add the service VLANs to upstream port 0/0/1.

```
huawei(config)#vlan 1001-1016 smart
huawei(config)#port vlan 1001-1016 0/0 1
```

Step 4 Add a service port.

Assume that the VDSL2 path mode is PTM mode, VLAN ID is 1001, port is 0/1/0, packets from the user VLAN are untagged, and service flow ID is 101. Add a service port as follows:

```
huawei(config)#service-port 101 vlan 1001 vdsl mode ptm 0/1/0 multi-service user-vlan untagged rx-cttr 8 tx-cttr 8
```

Step 5 Configure a VDSL2 line template.

This example uses the default VDSL2 line template (ID: 1).

Step 6 Configure a VDSL2 alarm template.

This example uses the default VDSL2 alarm template (ID: 1).

Step 7 Bind a VDSL2 line template and a VDSL2 alarm template, and activate the VDSL2 port.

For example, bind VDSL2 line template 1 and VDSL2 alarm template 1, and activate VDSL2 port 0/1/0.

```
huawei(config)#interface vdsl 0/1
huawei(config-if-vdsl-0/1)#deactivate 0
huawei(config-if-vdsl-0/1)#alarm-config 0 1
huawei(config-if-vdsl-0/1)#activate 0 template-index 1
```

----End

11.3.3.9 (Optional) Configuring Vectoring

Vectoring configurations on VDSL2 lines cancel the far-end crosstalk (FEXT) of VDSL2 lines to improve the line rate.

Context

For MA5623A/MA5616, when configuring vectoring, learn configuration item functions and configuration methods beforehand by referring to **Table 11-22**.

Copyright © Huawei Technologies Co., Ltd.

Table 11-22 Vectoring configuration items

Item	Function	Description	Commands
Global band plan	In the vectoring algorithm, the system requires that the upstream band and downstream band are separate from each other. Therefore, the band plan must be globally configured.	● The band plan can be globally configured only when vectoring is globally enabled. ● After vectoring is globally enabled, if the band plan configured for the line profile is incompatible with the band plan globally configured for vectoring and the upstream band plan and downstream band plan are not separate from each other, the port cannot be activated.	xdsl vectoring bandplan-type
Global vectoring configurations	Vectoring configurations take effect only when vectoring is globally enabled.	● Before enabling vectoring, globally configure the band plan. **NOTE** Services in a vectoring group port are interrupted when the vectoring function is enabled or disabled.	xdsl vectoring

Copyright © Huawei Technologies Co., Ltd.

Item	Function	Description	Commands
Vectoring profile	Configure the function of canceling the upstream and downstream crosstalk in the vectoring profile. After binding the configured vectoring profile to the ports, the system implements the vectoring algorithm on the ports in the vectoring group based on profile configurations.	By default, all ports are bound to vectoring profile 1. Default value: ● Upstream crosstalk cancelation: enable ● Downstream crosstalk cancelation: enable	Query a vectoring profile: display xdsl vectoring-profile
Policy for controlling frequent online and offline on ports	The Vectoring algorithm is executed every time a port in a Vectoring group goes online or offline. To prevent adverse impact on system functions due to long-term running Vectoring tasks caused by frequent online and offline on a port, set the policy for controlling frequent online and offline on ports based on site requirements.	By default, the policy for controlling frequent online and offline is set to limit.	xdsl frequently-retrain-control
Vectoring crosstalk matrix	The vectoring crosstalk matrix refers to crosstalk on a port in a vectoring group from other ports in the same vectoring group.	Before querying information about the vectoring crosstalk matrix, ensure that the global vectoring function is enabled and the specified port is in a vectoring group and activated.	display xdsl vectoring crosstalk-coupling-matrix

Copyright © Huawei Technologies Co., Ltd.

Item	Function	Description	Commands
Policy for activating a legacy customer premises equipment (CPE)	A legacy CPE is a VDSL2 CPE (supporting G.993.2, not G.993.5) that does not support Vectoring. If such a CPE is activated in G.993.2 mode in the Vectoring system, the crosstalk impact on other lines cannot be canceled, causing the Vectoring system performance to deteriorate. To minimize the impact, set the activation policy of a legacy CPE based on site requirements.	By default, the policy for activating a legacy CPE is set to limit. ● **no-limit**: The Vectoring legacy CPE is activated in common VDSL2 mode (G.993.2 mode), or non-Vectoring mode, in which the Vectoring system performance is affected. This mode is used in the Vectoring initial phase when a large number of CPEs need to be upgraded or replaced and the Vectoring performance are not concerned. ● **limit**: The Vectoring legacy CPE is activated in common VDSL2 mode but the line PSD is automatically shaped so that the CPE can be activated at a low VDSL2 rate, preventing crosstalk on other lines. This mode is used in Vectoring medium phase when some CPEs have not been upgrade or replaced. ● **force-friendly-ds-limit-us**: **force friendly** is used in the downstream	xdsl vectoring legacy-cpe activate-policy

Copyright © Huawei Technologies Co., Ltd.

Item	Function	Description	Commands
		direction and PSD automatic shaping is used in the upstream direction. ● **force-friendly-ds-no-limit-us**: **force friendly** is used in the downstream direction and no restriction is used in the upstream direction. ● **block**: The Vectoring legacy CPE cannot be activated in common VDSL2 mode. This mode is used in Vectoring mature phase when its performance is concerned and unnecessary crosstalk must be prevented.	

For MA5603T, when configuring vectoring, learn configuration item functions and configuration methods beforehand by referring to **Table 11-23**.

Copyright © Huawei Technologies Co., Ltd.

Table 11-23 Vectoring configuration items

Item	Function	Description	Commands
Global band plan	In the vectoring algorithm, the system requires that the upstream band and downstream band are separate from each other. Therefore, the band plan must be globally configured.	● The band plan can be globally configured only when vectoring is globally enabled. ● After vectoring is globally enabled, if the band plan configured for the line profile is incompatible with the band plan globally configured for vectoring and the upstream band plan and downstream band plan are not separate from each other, the port cannot be activated.	xdsl vectoring bandplan-type
Global vectoring configurations	Vectoring configurations take effect only when vectoring is globally enabled.	● Vectoring can be globally enabled only when devices are configured with VP boards. ● Before enabling vectoring, globally configure the band plan. **NOTE** Services in a vectoring group port are interrupted when the vectoring function is enabled or disabled.	xdsl vectoring

Copyright © Huawei Technologies Co., Ltd.

Item	Function	Description	Commands
Vectoring profile	Configure the function of canceling the upstream and downstream crosstalk in the vectoring profile. After binding the configured vectoring profile to the ports, the system implements the vectoring algorithm on the ports in the vectoring group based on profile configurations.	By default, all ports are bound to vectoring profile 1. Default value: ● Upstream crosstalk cancelation: enable ● Downstream crosstalk cancelation: enable	Commands: ● Add a vectoring profile: xdsl vectoring-profile add ● Modify a vectoring profile: xdsl vectoring-profile modify ● Delete a vectoring profile: xdsl vectoring-profile delete ● Query a vectoring profile: display xdsl vectoring-profile ● Bind a vectoring profile to the port: vectoring-config (VDSL mode)
Policy for controlling frequent online and offline on ports	The Vectoring algorithm is executed every time a port in a Vectoring group goes online or offline. To prevent adverse impact on system functions due to long-term running Vectoring tasks caused by frequent online and offline on a port, set the policy for controlling frequent online and offline on ports based on site requirements.	By default, the policy for controlling frequent online and offline is set to limit.	xdsl frequently-retrain-control

Copyright © Huawei Technologies Co., Ltd.

Item	Function	Description	Commands
Vectoring crosstalk matrix	The vectoring crosstalk matrix refers to crosstalk on a port in a vectoring group from other ports in the same vectoring group.	Before querying information about the vectoring crosstalk matrix, ensure that the global vectoring function is enabled and the specified port is in a vectoring group and activated.	display xdsl vectoring crosstalk-coupling-matrix

Copyright © Huawei Technologies Co., Ltd.

Item	Function	Description	Commands
Policy for activating a legacy customer premises equipment (CPE)	A legacy CPE is a VDSL2 CPE (supporting G. 993.2, not G. 993.5) that does not support Vectoring. If such a CPE is activated in G.993.2 mode in the Vectoring system, the crosstalk impact on other lines cannot be canceled, causing the Vectoring system performance to deteriorate. To minimize the impact, set the activation policy of a legacy CPE based on site requirements.	By default, the policy for activating a legacy CPE is set to limit. ● **no-limit**: The Vectoring legacy CPE is activated in common VDSL2 mode (G.993.2 mode), or non-Vectoring mode, in which the Vectoring system performance is affected. This mode is used in the Vectoring initial phase when a large number of CPEs need to be upgraded or replaced and the Vectoring performance are not concerned. ● **limit**: The Vectoring legacy CPE is activated in common VDSL2 mode but the line PSD is automatically shaped so that the CPE can be activated at a low VDSL2 rate, preventing crosstalk on other lines. This mode is used in Vectoring medium phase when some CPEs have not been upgrade or replaced. ● **force-friendly-ds-limit-us**: **force friendly** is used in the downstream	xdsl vectoring legacy-cpe activate-policy

Copyright © Huawei Technologies Co., Ltd.

Item	Function	Description	Commands
		direction and PSD automatic shaping is used in the upstream direction. ● **force-friendly-ds-no-limit-us**: **force friendly** is used in the downstream direction and no restriction is used in the upstream direction. ● **block**: The Vectoring legacy CPE cannot be activated in common VDSL2 mode. This mode is used in Vectoring mature phase when its performance is concerned and unnecessary crosstalk must be prevented.	

Data Plan

The **Table 11-24** lists key parameters of vectoring configurations.

Table 11-24 Key parameters of vectoring configurations

Item	Data	Description
Global vectoring configurations	enable	-
Global band plan	● Band plan type: 998ade ● USO type: type-a	-
Policy for activating a legacy customer premises equipment (CPE)	no-limit	The policy for activating a vectoring legacy CPE is configured as **no-limit** at the initial stage of vectoring application.

Copyright © Huawei Technologies Co., Ltd.

Item	Data	Description
Policy for controlling frequent online and offline on ports	no-limit	-
Vectoring group	Group ID: 1	All ports are added to the default vectoring group 1.
Vectoring profile	For the MA5623A/MA5616: Profile ID: 1 The upstream/ downstream crosstalk cancelation function in default Profile 1 are as follows: ● Upstream crosstalk cancelation: enable ● Downstream crosstalk cancelation: enable	-
	For MA5603T: ● Profile name: huawei ● Upstream crosstalk cancelation: enable ● Downstream crosstalk cancelation: enable ● The port to which a vectoring profile is bound: all ports on the0/1 board.	

NOTE

The Vectoring is configured on the ONU, and the configuration between the MA5623A/MA5616 and MA5603T is a little different, Here gives the configuring steps of MA5623A/MA5616 and MA5603T respectively.

Procedure

- Configuration procedure for the MA5623A/MA5616:
  1. Log in to the ONU remotely and start the configuration.

     By default, the user name is **root** and the password is **mduadmin**.
  2. Globally configure the band plan type.

     ```
     huawei(config)#xdsl vectoring bandplan-type 998ade us0-type type-a
     ```
  3. Configure the policy for activating a vectoring legacy CPE.

     ```
     huawei(config)#xdsl vectoring legacy-cpe activate-policy no-limit
     ```
  4. Configure the policy for controlling frequent online and offline on ports.

     ```
     huawei(config)#xdsl frequent-retrain-control 0/1/0 control-policy no-limit
     ```
  5. Enable global vectoring.

Copyright © Huawei Technologies Co., Ltd.

```
huawei(config)#xdsl vectoring enable
```

6. Save the data.

```
huawei(config)#save
```

- Configuration procedure for the MA5603T:

1. Log in to the ONU remotely and start the configuration.

   By default, the user name is **root** and the password is **admin**.

2. Globally configure the band plan type.

```
huawei(config)#xdsl vectoring bandplan-type 998ade us0-type type-a
```

3. Configure the vectoring profile as **huawei** and bind it to the VDSL2 port in the vectoring group.

```
huawei(config)#xdsl vectoring-profile add control enable enable name
huawei
huawei(config)#interface vdsl 0/1
huawei(config-if-vdsl-0/1)#vectoring-config all profile-name huawei
huawei(config-if-vdsl-0/1)#quit
```

4. Configure the policy for activating a vectoring legacy CPE.

```
huawei(config)#xdsl vectoring legacy-cpe activate-policy no-limit
```

5. Configure the policy for controlling frequent online and offline on ports.

```
huawei(config)#xdsl frequent-retrain-control 0/1/0 control-policy no-limit
```

6. Enable the global vectoring.

```
huawei(config)#xdsl vectoring enable
```

7. Save the data.

```
huawei(config)#save
```

----End

11.3.3.10 Configuring H.248 Voice Service (on the ONU)

This topic describes how to configure the voice service on the ONU based on the H.248 protocol to provide the high quality and low cost VoIP service for users.

Prerequisites

- The media gateway controller (MGC) interface data and the PSTN user data corresponding to the media gateway (MG) interface is configured on the MGC.
- Ensure that the **Status** of the voice board on the ONU is **Normal** by running the **display board 0** command.

Precautions

1. An ONU supports both the H.248 and SIP protocols; however, these two protocols are mutually exclusive. You can run the **display protocol support** command to query the currently supported voice protocol.
2. If the voice protocol needs to be switched, you need to delete the MG interface first and run the **protocol support** command to switch the protocol. After the configuration is complete, save the configuration and restart the system to make the configured protocol take effect.

Copyright © Huawei Technologies Co., Ltd.

CAUTION

This operation interrupts the ongoing services carried on the currently used MG interface. Hence, exercise caution when performing this operation.

Data plan

For details about the data plan, see **11.2.5 Principle of VoIP Service Data Plan**.

Item			Data
MG interface data **NOTE** The data configuration must be the same as the data configuration on the MGC.	Media and signaling parameters	Media and signaling upstream VLANs	200
		Media and signaling upstream port	0/0/1
		Media IP address and signaling IP address	10.10.10.10/24
		Default gateway IP address	10.10.10.1/24
	MG interface ID		0
	Signaling port ID		2944
	IP address of the primary MGC		200.200.200.200/24
	Port ID of the primary MGC		2944
	Coding		Text
	Transmission mode		UDP
	H248 version that MG starts to negotiate		1 (the negotiation starts from V1)
Voice user configuration data	Phone number		83110001-83110024
	Terminal identification		Terminal layering is not supported and the terminal identification ranges from 0 to 23.
	User priority		Cat2 for phone 1 Cat3 for phone 2 to phone 24 (default)
	User type		Common user (DEL user by default)
Common parameter	System parameter		Default value
	Overseas parameter		Default value
	PSTN port attribute		Polarity-reversal

Copyright © Huawei Technologies Co., Ltd.

Item		Data
	Ringing current attribute	Default value

Procedure

Step 1 Log in to and configure the ONU.

You can remote log in to the ONU from the OLT to perform the configuration. The user name is **root** and the password is **mduadmin**.

Step 2 Configure the upstream VLAN interface.

Specify the upstream VLAN interface for the media stream and the signaling flows and configure the IP addresses of the Layer 3 interface. These IP addresses are the sources of the IP address pools for the media stream and the signaling flows.

1. Create an upstream VLAN.

   The VLAN ID is 200 and the VLAN is a smart VLAN.

   ```
   huawei(config)#vlan 200 smart
   ```

2. Add the upstream port to the created upstream VLAN.

   Add upstream port 0/0/1 to VLAN 2000.

   ```
   huawei(config)#port vlan 200 0/0 1
   ```

3. Configure the IP address of the Layer 3 interface.

   Enter the VLAN interface mode and configure the lP address of the Layer 3 interface to 10.10.10.10

   ```
   huawei(config)#interface vlanif 200
   huawei(config-if-vlanif200)#ip address 10.10.10.10 24
   huawei(config-if-vlanif200)#quit
   ```

Step 3 Configure the media and signaling IP address pools.

Configure both the media IP address and signaling IP address to 10.10.10.10 and the MG IP address to 10.10.10.1.

```
huawei(config)#voip
huawei(config-voip)#ip address media 10.10.10.10 10.10.10.1
huawei(config-voip)#ip address signaling 10.10.10.10
huawei(config-voip)#quit
```

NOTE

- You can configure the attributes of the MG interface only when the media IP address and the signaling IP address exist in the media and signaling IP address pools.
- The media IP address can be different from the signaling IP address. Plan the data according to actual networking.

Step 4 Configure static routes.

Because the IP address of the VLAN interface and the IP address (200.200.200.200/24) of the MGC are in different network segments, you need to configure a route for the network segment from gateway 10.10.10.1 to 200.200.200.0.

```
huawei(config)#ip route-static 200.200.200.0 24 10.10.10.1
```

Step 5 Add an MG interface.

Copyright © Huawei Technologies Co., Ltd.

Add an MG interface to communicate with the MGC, which ensures that the MGC can control the call connection through the MG interface. Add MG interface 0 according to the data plan.

```
huawei(config)#interface h248 0
  Are you sure to add MG interface?(y/n)[n]:y
```

Step 6 Configure the attributes of the MG interface.

Pay attention to the following when configuring the attributes of the MG interface according to the data plan:

- The MG interface is registered by the IP address (default mode) or domain name, which must be the same as that on the MGC.
- The negotiated H.248 protocol version is V1, V2 or V3 (default value). The interface may fail to be registered because some softswitches do not support V3.

```
huawei(config-if-h248-0)#if-h248 attribute mgip 10.10.10.10 mgport
 2944 code text transfer udp primary-mgc-ip1 200.200.200.200 primary-mgc-port
 2944 mg-media-ip1 10.10.10.10 start-negotiate-version 1
```

Step 7 Reset the MG interface.

```
huawei(config-if-h248-0)#reset coldstart
  Are you sure to reset MG interface?(y/n)[n]:y
huawei(config-if-h248-0)#quit
```

NOTE

- You must cold reset the MG interface after configuring. Otherwise, the MG interface does not take effect.
- The MG interface can be cold reset only after parameters mgip, mgport, primary-mgc-ip1 (or mgc-domain-name1), mgcport_1, code, transfer, and mg-media-ip are correctly configured.

Step 8 Configure the PSTN user data.

Configure phone numbers of users 0/3/0-0/3/23 to 83110001-83110024 in batches and terminal identification to 0.

- Phone numbers are used for only internal emergency standalone, that is, internal extensions call each other. Actual phone numbers are assigned by the MGC.
- If the user of the MG interface is configured to support terminal layering, you need not configure the terminal identification because the system automatically allocates it. If the user of the MG interface does not support terminal layering, the terminal identification is mandatory. The terminal identification must be unique on one MG interface.

```
huawei(config)#esl user
huawei(config-esl-user)#mgpstnuser batadd 0/3/0 0/3/23 0 terminalid 0 telno
83110001
```

Step 9 Configure the call priority of a PSTN user.

```
huawei(config-esl-user)#mgpstnuser modify 0/3/0 priority cat2
huawei(config-esl-user)#quit
```

Step 10 Configure all the PSTN ports to support polarity reversal.

Configure the physical attributes of the PSTN port to which the users belong to support polarity reversal so that the user supports polarity reversal accounting.

```
huawei(config)#pstnport
huawei(config-pstnport)#pstnport attribute batset 0/3/0 0/3/23 reverse-pole-pulse
enable
huawei(config-pstnport)#quit
```

Step 11 Save the data.

Copyright © Huawei Technologies Co., Ltd.

```
huawei(config)#save
```

----End

11.3.3.11 Configuring SIP Voice Service (on the ONU)

This topic describes how to configure voice services based on the Session Initiation Protocol (SIP) on an optical network unit (ONU). The voice over IP (VoIP) services have high quality, but require low cost.

Prerequisites

- The IP Multimedia Subsystem (IMS) interface data and public switched telephone network (PSTN) user data corresponding to the SIP interface is configured on the IMS.
- **Status** of the voice board on the ONU is normal. (To verify board status, run the **display board 0** command.)

Precautions

1. An ONU supports both the H.248 and SIP protocols; however, these two protocols are mutually exclusive. You can run the **display protocol support** command to query the currently supported voice protocol.
2. If the voice protocol needs to be switched, you need to delete the MG interface first and run the **protocol support** command to switch the protocol. After the configuration is complete, save the configuration and restart the system to make the configured protocol take effect.

CAUTION

This operation interrupts the ongoing services carried on the currently used MG interface. Hence, exercise caution when performing this operation.

Data Plan

For configuration rules and description of configuration items, see **11.2.5 Principle of VoIP Service Data Plan**.

Item			Data
SIP interface data **NOTE** (It must be the same as that on the IMS core network device.)	Media and signaling parameters	Media and signaling upstream VLAN	200
		Media and signaling upstream port	0/0/1
		Media IP address and signaling IP address	10.10.10.10/24

Copyright © Huawei Technologies Co., Ltd.

Item			Data
		Default gateway IP address	10.10.10.1/24
	SIP interface ID		0
	Signaling port ID		5060
	IP address of the main IMS equipment		200.200.200.200/24
	Port ID of the main IMS equipment		5060
	Coding scheme		Text
	Transmission mode		UDP
	Home domain name (SIP)		huawei
	Profile index (SIP)		1
Voice user configuration data	Phone number		83110001-83110024
	User priority		Phone 1 indicates Cat2. Phone 2 to phone 24 indicate Cat3 (default value).
	User type		Common user (the DEL user by default)
Common Parameter	System parameter		Default value
	Overseas parameter		Default value
	PSTN port attribute		Polarity-Reversing Pulse
	Ringing current attribute		Default value

Procedure

Step 1 Log in to and configure the ONU.

You can remote log in to the ONU from the OLT to perform the configuration. The user name is **root** and the password is **mduadmin**.

Step 2 Configure the upstream VLAN interface.

Specify the upstream VLAN interface for the media stream and the signaling flows and configure the IP addresses of the Layer 3 interface. These IP addresses are the sources of the IP address pools for the media stream and the signaling flows.

1. Create an upstream VLAN.

   The VLAN ID is 200 and the VLAN is a smart VLAN.

   ```
   huawei(config)#vlan 200 smart
   ```


Copyright © Huawei Technologies Co., Ltd.

2. Add the upstream port to the created upstream VLAN.

   Add upstream port 0/0/1 to VLAN 2000.

   ```
   huawei(config)#port vlan 200 0/0 1
   ```

3. Configure the IP address of the Layer 3 interface.

   Enter the VLAN interface mode and configure the lP address of the Layer 3 interface to 10.10.10.10

   ```
   huawei(config)#interface vlanif 200
   huawei(config-if-vlanif200)#ip address 10.10.10.10 24
   huawei(config-if-vlanif200)#quit
   ```

Step 3 Configure the media and signaling IP address pools.

Set the media IP address and signaling IP address to 10.10.10.10, and the media gateway to 10.10.10.1.

```
huawei(config)#voip
huawei(config-voip)#ip address media 10.10.10.10 10.10.10.1
huawei(config-voip)#ip address signaling 10.10.10.10
huawei(config-voip)#quit
```

NOTE

- Attributes of the MG interface can be configured only when the media IP address and the signaling IP address exist in the media and signaling IP address pools.
- The Media IP address and signaling IP address can be different. Data planning should be based on networking requirements.

Step 4 Configure static routes.

Because the IP address of the VLAN interface and that of the IMS (200.200.200.200/24) are in different network segments, the configured routes must be from gateway 10.10.10.1 to the network segment 200.200.200.0.

```
huawei(config)#ip route-static 200.200.200.0 24 10.10.10.1
```

Step 5 Add an SIP interface.

The SIP interface is used for IMS communication.

```
huawei(config)#interface sip 0
  Are you sure to add the SIP interface?(y/n)[n]:y
```

Step 6 Configure the basic attributes of the SIP interface.

```
huawei(config-if-sip-0)#if-sip attribute basic media-ip 10.10.10.10 signal-ip
 10.10.10.10 signal-port 5060 transfer udp primary-proxy-ip1 200.200.200.200
 primary-proxy-port 5060 home-domain huawei sipprofile-index 1
```

Step 7 (Optional) Configure the optional attributes of the SIP interface.

Run the **if-sip attribute optional** command to configure the optional attributes, including the domain name, description, register server uniform resource identifier (URI), phone context, and conference factory URI of the SIP interface.

Step 8 Reset the SIP interface.

```
huawei(config-if-sip-0)#reset
  Are you sure to reset the SIP interface?(y/n)[n]:y
huawei(config-if-sip-0)#quit
```

Step 9 Configure the SIP PSTN user data.

Configure in batches the phone numbers of users 0/3/0-0/3/23 to 83110001-83110024.

Copyright © Huawei Technologies Co., Ltd.

NOTE

- To configure the data of a single SIP PSTN user, run the **sippstnuser add** command.
- To configure the data of multiple SIP PSTN users in batches, run the **sippstnuser batadd** command.

```
huawei(config)#esl user
huawei(config-esl-user)#sippstnuser batadd 0/3/0 0/3/23 0 telno 83110001
```

Step 10 Configure call priorities for SIP PSTN users.

```
huawei(config-esl-user)#sippstnuser attribute set 0/3/0 priority cat2
huawei(config-esl-user)#quit
```

Step 11 Configure all the PSTN ports to support polarity reversal.

Configure the physical attributes of the PSTN port to which the users belong to support polarity reversal so that the user supports polarity reversal accounting.

```
huawei(config)#pstnport
huawei(config-pstnport)#pstnport attribute batset 0/3/0 0/3/23 reverse-pole-pulse
enable
huawei(config-pstnport)#quit
```

Step 12 Save the data.

```
huawei(config)#save
```

----End

11.3.3.12 Configuring the IPTV Service (on the ONU)

This topic describes how to configure the video on demand (VoD) service and multicast service for home gateway (HGW) users on an optical network unit (ONU) when HGWs are connected upstream to the ONU through local area networks (LANs) or in xDSL mode.

Data Plan

The following table provides key information about the IPTV service.

Item	Data	Remarks
Traffic profile	ID: 10 CIR: off VLAN priority: 4 Downstream priority policy: local-setting	-
User VLAN in the scenario in which HGWs are upstream connected to an ONU through LANs	User VLAN ID: 1, 2, 3...	HGWs can send untagged packets or packets with user VLAN tags.

Copyright © Huawei Technologies Co., Ltd.

Item	Data	Remarks
VPI/VCI of ADSL2+ users in the scenario in which HGWs are connected upstream to an ONU in ADSL2+ mode	VPI: 0 VCI: 35	Internet service providers (ISPs) provide VPI/VCI information.
VDSL2 path mode in the scenario in which HGWs are connected upstream to an ONU in VDSL2 mode	PTM	Both the central office and HGWs must support the PTM mode.
VLAN ID of the VoD service	300	The VoD service is a carrier-operating, closed service and primarily adopts only SVLAN tags, which are transparently transmitted by OLTs.
Multicast VLAN ID of the ONU	1000	-
Multicast VLAN ID of HGWs	43	A carrier generally specifies a globally unique multicast VLAN ID for HGWs.

Procedure

- Configure the VoD service.

  Create VLAN 300 with the common attribute and add upstream port 0/0/1 to the VLAN.

  ```
  huawei(config)#vlan 300 smart
  huawei(config)#port vlan 300 0/0 1
  ```

  Configure a traffic profile for the IPTV service.

  The IEEE 802.1p priority of the IPTV service is 4, and rate limitation is not required. To check whether any existing traffic profile meets the requirements, run the **display traffic table ip** command. In this example, the query result shows that no traffic profile meets the requirements, so a traffic profile needs to be configured.

Copyright © Huawei Technologies Co., Ltd.

Add traffic profile 10 and set *priority-policy* to **local-setting**. Then, traffic is scheduled based on the priority specified in the traffic profile.

```
huawei(config)#traffic table ip index 10 cir off priority 4 priority-policy
local-setting
```

Configure a service flow for the VoD service.

Configurations vary according to upstream interface types of HGWs.

- If HGWs are connected to an ONU upstream through LANs and upstream packets contain user VLAN tags, the ONU needs to perform a switch between user VLAN IDs and SVLAN IDs.

  Assume that the user VLAN ID is 1 and the Ethernet port is 0/3/1. Add a service flow as follows:

  ```
  huawei(config)#service-port 301 vlan 300 eth 0/3/1 multi-service user-vlan
  1 rx-cttr 10 tx-cttr 10
  ```

- If HGWs are connected to an ONU upstream in ADSL2+ mode, upstream packets contain users' PVC information so the ONU needs to perform a switch between PVC information and SVLAN IDs.

  Assume that the VPI/VCI is 0/35 and the ADSL2+ port is 0/2/0. Add a service flow as follows:

  ```
  huawei(config)#service-port 301 vlan 300 adsl vpi 0 vci 35 0/2/0 multi-
  service user-vlan untagged rx-cttr 10 tx-cttr 10
  ```

- If HGWs are connected to an ONU upstream in VDSL2 mode, formats of upstream packets depend on the encapsulation mode.

  Assume that the VDSL2 path mode is PTM mode, port is 0/1/0, and packets from the user VLAN are untagged. Add a service flow as follows:

  ```
  huawei(config)#service-port 301 vlan 300 vdsl mode ptm 0/1/0 multi-service
  user-vlan untagged rx-cttr 10 tx-cttr 10
  ```

- Configure the multicast service.

  Create multicast VLAN 1000 with the common attribute and add upstream port 0/0/1 to the multicast VLAN.

  ```
  huawei(config)#vlan 1000 smart
  huawei(config)#port vlan 1000 0/0 1
  ```

  Set the IGMP version to IGMP v3.

  ```
  huawei(config)#multicast-vlan 1000
  huawei(config-mvlan1000)#igmp version v3
  ```

  Set the IGMP mode to IGMP proxy.

  ```
  huawei(config-mvlan1000)#igmp mode proxy
    Are you sure to change IGMP mode?(y/n)[n]:y
  ```

  Configure an IGMP upstream port.

  ```
  huawei(config-mvlan1000)#igmp uplink-port 0/0/1
  ```

  Configure a program library. Set the multicast IP address range to 224.1.1.10-224.1.1.100 and the IP address of the multicast server to 10.10.10.10.

  ```
  huawei(config-mvlan1000)#igmp program add batch ip 224.1.1.10 to-ip
  224.1.1.100 sourceip 10.10.10.10
  huawei(config-mvlan1000)#quit
  ```


Copyright © Huawei Technologies Co., Ltd.

Configure a service flow for the multicast service.

Configurations vary according to upstream interface types of HGWs.

- If HGWs are connected to an ONU upstream through LANs, assume that the user VLAN ID is 43 and the Ethernet port is 0/3/1, and add a service flow as follows:
  ```
  huawei(config)#service-port 401 vlan 1000 eth 0/3/1 multi-service user-vlan 43 rx-cttr 10 tx-cttr 10
  ```
- If HGWs are connected to an ONU upstream in ADSL2+ mode, assume that the VPI/VCI is 0/35 and the ADSL2+ port is 0/2/0, and add a service flow as follows:
  ```
  huawei(config)#service-port 401 vlan 1000 adsl vpi 0 vci 35 0/2/0 multi-service user-vlan untagged rx-cttr 10 tx-cttr 10
  ```
- If HGWs are connected to an ONU upstream in VDSL2 mode, assume that the VDSL2 path mode is PTM mode, the user VLAN ID is 43, and the VDSL2 port is 0/1/0, and add a service flow as follows:
  ```
  huawei(config)#service-port 401 vlan 1000 vdsl mode ptm 0/1/0 multi-service user-vlan 43 rx-cttr 10 tx-cttr 10
  ```

Configure a multicast user and add the user to the multicast VLAN.

Configure service flow 401 as a multicast user, add the user to multicast VLAN 1000, and adopt the no-auth mode for the multicast user.

```
huawei(config-mvlan1000)#btv
huawei(config-btv)#igmp user add service-port 401 no-auth
huawei(config-btv)#multicast-vlan 1000
huawei(config-mvlan1000)#igmp multicast-vlan member service-port 401
huawei(config-mvlan1000)#quit
```

----End

11.3.3.13 Configuring Link Aggregation, Congestion Control, and Security Policy

The global configuration of upstream link aggregation and queue scheduling based on priorities ensures service reliability. The global configuration of security policies ensures service security.

Context

Link aggregation provides a higher bandwidth and uplink reliability for optical line terminals (OLTs) by aggregating multiple uplink Ethernet ports to one link aggregation group (LAG). Link aggregation is recommended.

Congestion control places the packets to be sent from a port into multiple queues that are marked with different priorities. Then, the packets are sent based on queue priorities. Congestion control is recommended.

Security policies ensure system, user, and service security.

NOTE

Enable a service security function based on the service type. For details, see **11.2.7 Principle of Security Data Plan**.

Procedure

- Configure link aggregation.

  The following configurations are used as an example to configure link aggregation:

  - Uplink ports 0/19/0 and 0/19/1 are added to a LAG.

Copyright © Huawei Technologies Co., Ltd.

- The two ports send packets upstream based on the packets' source MAC addresses.
- The LAG works in Link Aggregation Control Protocol (LACP) static aggregation mode.

```
huawei(config)#link-aggregation 0/19 0-1 ingress workmode lacp-static
```

- Configure queue scheduling.

  According to quality of service (QoS) planning principles, all packets are scheduled in strict priority (SP) mode and mapped to queues according to the packets' priorities. For details about QoS planning principles, see **11.2.2 Principle of QoS Data Plan**.

```
huawei(config)#queue-scheduler strict-priority
huawei(config)#cos-queue-map cos0 0 cos4 4 cos5 5 cos6 6
```

- Configure system security.
  - Enable deny of service (DoS) anti-attack on both the OLT and optical network units (ONUs).
    1. Run the **security anti-dos enable** command to globally enable DoS anti-attack.
    2. Run the **security anti-dos control-packet policy** command to configure a protocol packet processing policy that will be used when a DoS attack occurs.
    3. Run the **security anti-dos control-packet rate** command to configure the threshold for the rate of sending protocol packets to the CPU.
  - Enable IP address anti-attack on both the OLT and ONUs.

    Run the **security anti-ipattack enable** command to enable IP address anti-attack.
- Configure user security.
  - Enable MAC address anti-flapping on both the OLT and ONUs.

    Run the **security anti-macduplicate enable** command to enable MAC address anti-flapping.
  - Enable MAC address anti-spoofing on both the OLT and ONUs.
    1. In global config mode, run the **security anti-macspoofing enable** command to globally enable MAC address anti-spoofing.
    2. Enable MAC address anti-spoofing at VLAN level in global config mode or service profile mode:
       a. In global config mode, run the **security anti-macspoofing vlan** command to enable MAC address anti-spoofing.
       b. Perform the following operations to enable MAC address anti-spoofing in service profile mode:
          a. In global config mode, run the **vlan service-profile** command to create a VLAN service profile.
          b. Run the **security anti-macspoofing enable** command to enable MAC address anti-spoofing at VLAN level.
          c. Run the **commit** command to make the profile configuration take effect.
          d. Run the **quit** command to quit the VLAN service profile mode.
          e. Run the **vlan bind service-profile** command to bind the created VLAN service profile to a VLAN.
    3. (Optional) Run the **security anti-macspoofing max-mac-count** command to set the maximum number of MAC addresses that can be bound to a service flow.

Copyright © Huawei Technologies Co., Ltd.

4. (Optional) Run the **security anti-macspoofing exclude** command to configure the types of packets for which MAC address anti-spoofing does not take effect, such as Internet Group Management Protocol (IGMP) packets.

- Enable IP address anti-spoofing on ONUs.

  IP address anti-spoofing can be enabled or disabled at three levels: global, VLAN, and service port levels. This function takes effect only after it is enabled at the three levels. Among the three levels, IP address anti-spoofing is disabled only at the global level by default.

  1. In global config mode, run the **security anti-ipspoofing enable** command to enable IP address anti-spoofing at the global level.
  2. In VLAN service profile mode, run the **security anti-ipspoofing enable** command to enable IP address anti-spoofing at the VLAN level.
  3. Run the **security anti-ipspoofing service-port** *serviceport-id* **enable** command to enable IP address anti-spoofing at the service port level.

- Configure service security.
  - Enable Dynamic Host Configuration Protocol (DHCP) Option 82 on both the OLT and ONUs. This configuration is recommended for the DHCP-based Internet access service.

    1. Enable DHCP Option 82 on both the OLT and ONUs.

       DHCP Option 82 can be enabled or disabled at four levels: global, port, VLAN, and service port levels. This function takes effect only after it is enabled at the four levels. Among the four levels, DHCP Option 82 is disabled only at the global level by default.

       - The global level: In global config mode, run the **dhcp option82** command to enable DHCP Option 82 at the global level.

         When you run this command, select the **enable**, **forward**, or **rebuild** parameter based on site requirements. The three parameters can all enable DHCP Option 82 but provide different packet processing policies on the OLT. For details, see the **dhcp option82** command.

       - The port level: In global config mode, run the **dhcp option82 port** or **dhcp option82 board** command to enable DHCP Option 82 at the port level.
       - The VLAN level:

         a. In global config mode, run the **vlan service-profile** command to create a VLAN service profile.
         b. Run the **dhcp option82 enable** command to enable DHCP Option 82 at the VLAN level.
         c. Run the **commit** command to make the profile configuration take effect.
         d. Run the **quit** command to quit the VLAN service profile mode.
         e. Run the **vlan bind service-profile** command to bind the created VLAN service profile to a VLAN.

       - The service port level: In global config mode, run the **dhcp option82 service-port** command to enable DHCP Option 82 at the service port level.

Copyright © Huawei Technologies Co., Ltd.

2. On the OLT, run the **dhcp-option82 permit-forwarding service-port** command with the **enable** parameter selected, to allow ONU DHCP packets to carry Option 82 information.

- Enable Policy Information Transfer Protocol (PITP) on both the OLT and ONUs. This configuration is recommended for the PPPoE-based Internet access service.

  1. Enable PITP on both the OLT and ONUs.

     PITP can be enabled or disabled at four levels: global, port, VLAN, and service port levels. This function takes effect only after it is enabled at the four levels. Among the four levels, PITP is disabled only at the global level by default.

     - The global level: In global config mode, run the **pitp enable pmode**, **pitp forward pmode**, or **pitp rebuild pmode** command to enable PITP at the global level.

       In the preceding commands, the **enable**, **forward**, and **rebuild** parameters can all enable PITP but provide different packet processing policies on the OLT. Select one of them based on site requirements. For details, see the **pitp** command.
     - The port level: In global config mode, run the **pitp port** or **pitp board** command to enable PITP at the port level.
     - The VLAN level:

       a. In global config mode, run the **vlan service-profile** command to create a VLAN service profile.

       b. Run the **pitp enable** command to enable PITP at the VLAN level.

       c. Run the **commit** command to make the profile configuration take effect.

       d. Run the **quit** command to quit the VLAN service profile mode.

       e. Run the **vlan bind service-profile** command to bind the created VLAN service profile to a VLAN.
     - The service port level: In global config mode, run the **pitp service-port** command to enable PITP at the service port level.

  2. On the OLT, run the **pitp permit-forwarding service-port** command with the **enable** parameter selected, to allow ONU PPPoE packets to carry a vendor tag.

----End

11.3.3.14 Configuring the Internet Access Service (on the HGW)

This topic describes how to configure the Internet access service for residential users on a home gateway (HGW) when the HGW is connected to an ONU upstream through a local area network (LAN) or in xDSL mode.

Context

Residential users generally access the Internet in Point-to-Point Protocol over Ethernet (PPPoE) dial-up mode. PPPoE dial-up can be performed on personal computers (PCs) or HGWs.

The configuration processes on HGWs of different models or in different appearances are similar. This topic describes how to configure the Internet access service on an HG239 that is connected to an ONU upstream through a LAN and on an HG527 that is connected to an ONU upstream in ADSL2+ mode.

Copyright © Huawei Technologies Co., Ltd.

Procedure

- Configure the Internet access service (on an HG239).
  1. Log in to the Web configuration window.
     a. Enter http://192.168.1.1/cu.html (default IP address) to the address bar of the Internet Explorer (IE) and press Enter.
     b. In the login dialog box, enter the user name and password of the administrator (the Internet service provider (ISP) provides the default user name and default password). Then, click **OK**.
  2. Set parameters for the Internet access service.

     Assume that ports LAN1 and LAN2 are Internet access ports for PCs.
     a. Choose **Network** > **Bandwidth Configuration** from the navigation tree.
     b. Create WAN connection 1 and set parameters based on the following table.

Parameter	Value
Bearing service	INTERNET
VLAN enabling	Enabled: Upstream packets contain VLAN tags. Disabled: Upstream packets do not contain VLAN tags. **NOTE** If **uservlan** is set to **untagged** when you configure a service flow for the Internet access service on the ONU, set this parameter to **Disabled**; otherwise, set it to **Enabled**.
VLANID [1-4094]	If **VLAN enabling** is set to **Enabled**, this parameter takes the value of **uservlan** that is specified when you configure a service flow for the Internet access service on the ONU.
Binding item	LAN1 and LAN2: PCs connected to ports LAN1 and LAN2 can simultaneously access the Internet.
Mode	Bridge: PCs access the Internet in PPPoE dial-up mode.

     c. Click **OK**.
  3. Restart the HGW.

     Choose **Management** > **Device Management** and click **Restarting the Device**.
- Configure the Internet access service (on an HG527).
  1. Log in to the Web configuration window.
     a. Enter http://192.168.1.1/cnc.html (default IP address) to the address bar of the IE and press Enter.
     b. In the login dialog box, enter the user name (default: admin) and password (default: admin) of the administrator. Then, click **OK**.
  2. Set parameters for the Internet access service.

     Assume that ports LAN1 and LAN2 are Internet access ports for PCs.
     a. Choose **Network** > **Bandwidth Configuration** from the navigation tree.

Copyright © Huawei Technologies Co., Ltd.

b. Create WAN connection 1 and set parameters based on the following table.

Parameter	Value
Bearing service	INTERNET
Enabling	If this parameter is selected, WAN connection 1 is used.
VPI/VCI	Contact your carrier for the value ranges of VPIs and VCIs. Ensure that the VPI/VCI setting (for example, 0/35) on an HGW is consistent with that on the office to which the HGW is connected.
Binding item	LAN1 and LAN2: PCs connected to ports LAN1 and LAN2 can simultaneously access the Internet.
Mode	Bridge: PCs access the Internet in PPPoE dialup mode.
Encapsulation mode	LLC

c. Click **OK**.

3. Restart the HGW.

   Choose **Management** > **Device Management** and click **Restarting the Device**.

----End

11.3.3.15 Configuring the IPTV Service (on the HGW)

This topic describes how to configure the IPTV service on the HGW that uses LAN or xDSL for upstream transmission. This configuration enables home subscribers to watch IPTV programs using STBs and TVs.

Context

HGWs have different models and appearances but their configuration procedures are similar. This topic uses the HG239 that uses LAN for upstream transmission and the HG527 that uses ADSL2+ for upstream transmission as examples.

Procedure

- Configure the IPTV service on the HG239.
  1. Log in to the Web configuration window.
     a. Enter http://192.168.1.1/cu.html (default IP address) to the address bar of the Internet Explorer (IE) and press Enter.
     b. In the login dialog box, enter the user name and password of the administrator (the Internet service provider (ISP) provides the default user name and default password). Then, click **OK**.
  2. Configure multicast parameters.

     This example assumes LAN 4 as an IPTV port.

Copyright © Huawei Technologies Co., Ltd.

a. Choose **Network** > **Bandwidth Configuration** from the navigation tree.

b. In the right pane, create LAN connection 2 for the IPTV service. Set the parameters as follows:

Parameter	Value
Bearing service	**OTHER**: The connection is used for the IPTV service.
VLAN enabling	**Enable** VLAN tags are added to upstream packets. **NOTE** When multicast service flows are created on the ONU, the value is **Disable** if **uservlan** is untagged and the value is **Enable** if **uservlan** is tagged.
VLANID [1-4094]	Multicast VLAN ID corresponding to the user VLAN value for multicast service flows created on the ONU. In this example, set this parameter to 43.
Binding item	LAN4
Mode	Bridge
DHCP transparent transmission	Enable

c. Click **OK** to save the settings.

3. Restart the HGW.

   Choose **Management** > **Device Management** and click **Restarting the Device**.

- Configure the IPTV service on the HG527.

1. Log in to the Web configuration window.

   a. Enter http://192.168.1.1/cnc.html (default IP address) to the address bar of the IE and press Enter.

   b. In the login dialog box, enter the user name (default: admin) and password (default: admin) of the administrator. Then, click **OK**.

2. Configure multicast parameters.

   This example assumes LAN 4 as an IPTV port.

   a. Choose **Network** > **Bandwidth Configuration** from the navigation tree.

   b. In the right pane, create LAN connection 1 for dialup Internet access services. Set the parameters as follows:

Parameter	Value
Bearing service	**OTHER**: The connection is used for the IPTV service.
Enabling	The LAN connection is enabled when this check box is selected.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Value
VLAN enabling	**Enable**: VLAN tags are added to upstream packets. **NOTE** When multicast service flows are created on the ONU, the value is **Disable** if **uservlan** is untagged and the value is **Enable** if **uservlan** is tagged.
VLANID [1-4094]	Multicast VLAN ID on the HGW when multicast service flows are created on the ONU. In this example, set this parameter to **43**.
VPI/VCI	Set the VPI/VCI to the same as that configured on the devices at the central office. In this example, set this parameter to **0/35**.
Binding item	LAN4
Mode	Bridge
Encapsulation mode	LLC

c. Click **OK** to save the settings.

3. Restart the HGW.

   Choose **Management** > **Device Management** and click **Restarting the Device**.

----End

11.3.3.16 Verifying Services

This topic describes how to verify service configurations in the FTTB+HGW networking (ONU providing the VoIP service). In this scenario, the ONUs are placed in the building far away from the central office. The ONUs provide remote service verification methods including PPPoE dialup emulation, call emulation, and multicast emulation for configuration and commissioning engineers to verify services remotely after services are configured.

Prerequisites

ONUs and upper-layer devices have been connected properly. The BRAS and MGC/IMS have been configured.

Background Information

The following table lists the remote verification methods for different services.

NOTE

Currently, the VoD service does not support remote verification.

Copyright © Huawei Technologies Co., Ltd.

Remote Service Verification Method	Function	Remarks
PPPoE dialup emulation	An ONT emulates PPPoE user terminal software to perform dialup and interact with the BRAS to verify the connectivity between the ONT and BRAS.	PPPoE dialup emulation requires a service flow which does not belong to a QinQ VLAN. A user name, password, and authentication mode must be configured on the BRAS for the PPPoE dialup emulation. An ONU supports a maximum of one PPPoE dialup emulation.
Call emulation	An ONT emulates a VoIP user to make a call to check whether the VoIP service data is correctly configured. You can also use the call emulation function to locate a fault when the VoIP service is faulty.	● An ONU can emulate the caller or callee in a call to a phone. Therefore, a functioning phone is required in the central office where the acceptance personnel is. ● An ONU can emulate the caller and callee simultaneously in an emulation test. No phone is required in the test. ● An ONU supports a maximum of one call emulation.
Multicast emulation	This function enables you to emulate a multicast user going online and lead the program stream to an ONU. By querying the real-time traffic of the multicast program, you can check whether the multicast function is performing well.	The multicast service that is configured in the dynamic controllable multicast mode does not support remote verification.

Data plan

Item	Data	Remarks
PPPoE dialup emulation parameter	Service flow ID: 101 Emulation timeout time: 10s	The entered user name, password, and authentication mode must be consistent with those configured on the BRAS.

Copyright © Huawei Technologies Co., Ltd.

Item	Data	Remarks
Call emulation parameter	Caller port: 0/3/0 Callee port: 0/3/23 Callee telephone number: 83110024	The ONU emulates the caller and callee at the same time using the default emulation parameters. You can view the parameters by running the **display pots emulational configuration** command.
Multicast emulation parameter	Multicast service flow ID: 401 Multicast VLAN: 1000 IP address of the multicast program: 224.1.1.10	-

Procedure

- Verify the Internet access service using PPPoE dialup emulation.
  1. Start an emulation test by running the **simulate dhcp start** command.

```
huawei(config)#pppoe simulate start
  Command:
          pppoe simulate start
 Service-port(index<0-999>):101
 User Name(length<1,65>):user0
 User Password(length<0,16>):*******
 Authentication Mode:
 1. Chap  2. Pap [default 1]:1
 Overtime Time(5-60s)[default 5]:10
```

  2. Query the emulation test information by running the **display pppoe simulate info** command.

```
huawei(config)#display pppoe simulate info
  PPPoE simulate information is:
  ------------------------------------------------------------------
  Service-port:  101
  User name:     user0
  Current phase: -                     //*Emulation phase
  Result:        Success               //*Emulation result
  Start time:    2011-11-16 15:41:29+08:00
  End time:      2011-11-16 15:41:34+08:00
  Session ID:    591
  User IP:       192.168.50.2
  Gateway IP:    192.168.50.254
  ------------------------------------------------------------------
```

  3. Terminate the emulation test by running the **simulate dhcp start** command.

```
huawei(config)#pppoe simulate stop
```

- Verify the voice service using call emulation.
  1. Start an emulation test by running the **ont emulational call** command.

```
huawei(config)#test
huawei(config-test)#pots emulational-call caller-port 0/3/0 callee-port
0/3/23 callee-telno 83110024
```

  2. The ONU outputs the call emulation result after the test is complete.

     The ONU outputs the call emulation result and failure of the cause if the emulation test fails.

Copyright © Huawei Technologies Co., Ltd.

```
huawei(config-test)#
  Caller port               :  0/3/0
  Callee port               :  0/3/23
  Test result               :  Test Succeed
```

- Verify the multicast service using multicast emulation.
  1. Run the **igmp static-join** command to order a multicast program by emulating a multicast user.

     ```
     huawei(config)#btv
     huawei(config-btv)#igmp static-join service-port 401 ip 224.1.1.10 vlan
     1000
     ```

  2. Run the **display igmp use** command to query the status of the multicast user.

     ```
     huawei(config-btv)#display igmp user service-port 401
       User                      : 0/3/1 //*Use an ETH port as an example.
       State                     : online
       Authentication            : no-auth
       Quick leave               : MAC-based
       IGMP flow ID              : 0
       Video flow ID             : 0
       Log switch                : enable
       Bind profiles             : -
       IGMP version              : IGMP v3
       Available programs        : 91
       Global Leave              : disable
       User MaxBandWidth         : no-limit
       Used bandwidth(kbps)      : 5000
       The percentage of used
       bandwidth to port rate(%) : -
       Total video bandwidth     : -
       Mcast video bandwidth     : -
       Active program list

     ------------------------------------------------------------------------
     --
       Program name     VLAN  IP/MAC           State           Start-time

     ------------------------------------------------------------------------
     --
       program1         1000  224.1.1.10       watching        2011-07-13
                                                               14:41:18

     ------------------------------------------------------------------------
     --
       Total: 1
     ```

  3. Run the **display multicast flow-statistic** command to query the real-time traffic of the multicast program.

     ```
     huawei(config-btv)#display multicast flow-statistic ip 224.1.1.10 vlan
     1000
       Command is being executed, please wait...
       Multicast flow statistic result: 360(kbps)
     ```

- Verify the VoD service.
  1. Run the **display mac-address service-port** command on the ONU to query learned MAC addresses of VoD users. The learned MAC addresses of VoD users indicate that services are functioning properly between the ONU and VoD users.

     If the VPI/VCI is 0/35 and the ADSL2+ port is 0/2/0, run the following command to query the learned MAC addresses of VoD users:

     ```
     huawei(config)#display mac-address service-port 301

       Command:
              display mac-address service-port 301
     ```


Copyright © Huawei Technologies Co., Ltd.

```
-----------------------------------------------------------------------
-
  SRV-P BUNDLE TYPE MAC            MAC TYPE F /S /P  VPI  VCI
VLANID
  INDEX INDEX

-----------------------------------------------------------------------
-
    301    -   adl 1010-1010-1000  dynamic  0 /2 /0  0    35          300

-----------------------------------------------------------------------
-
  Total: 1
  Note: F--Frame, S--Slot, P--Port,
        VPI indicates ONT ID for PON, VCI indicates GEM index for GPON,
        v/e--vlan/encap, pri-tag--priority-tagged,
        ppp--pppoe, ip--ipoe, ip6--ipv6oe
```

2. On the OLT, run the **display mac-address vlan** command to query the learned ONU MAC addresses. The learned ONU MAC addresses indicate that services are functioning properly between the OLT and ONUs.

----End

11.3.4 FTTB/FTTC+HGW Networking (HGW Providing the VoIP Service)

In an FTTB/FTTC+HGW network, the HGW provides the Internet access and IPTV services. In addition, the built-in IAD of the HGW provides the VoIP service by connecting to the upstream ONU using LAN or xDSL.

11.3.4.1 Service Requirements and Application Scenario

Service Requirements

A gigabit-capable passive optical network (GPON) should be capable of delivering triple play service over Category 5 cables or twisted pairs. Service requirements are described as follows:

- Sharing of Internet access among multiple computers in the household
- Access of multiple phones in the household
- Internet Protocol (IPTV) services (program preview or watch) enabled by set-top boxes (STB)
- Independent provisioning of Internet access, voice, and IPTV services
- Ensured service security:
  - Internet access services protected against unauthorized access, hijacking or unauthorized borrowing of user accounts, MAC/IP spoofing, and malicious attack
  - Voice and IPTV services protected against MAC/IP spoofing, malicious attack, and traffic flooding attack
- Easy fault location and service maintenance

Application Scenario

Figure 11-9 shows a GPON FTTB+HGW network. The GPON OLT is deployed at the central office and connects to the MAN using aggregation, and the ONU is deployed in the buildings

Copyright © Huawei Technologies Co., Ltd.

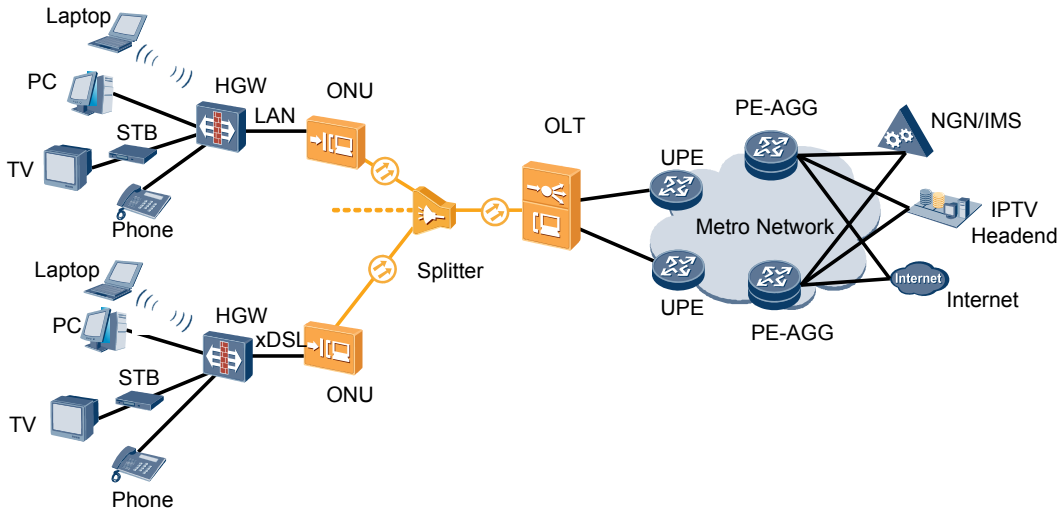
or street fiber distribution terminals. Access interfaces are deployed on the HGW that connects to the ONU using LAN or xDSL.

- The HGW connects to the upstream ONU through the Ethernet or xDSL port and provides the Internet access service through the FE or Wi-Fi port and the IPTV service through the FE port in the downstream direction.
- The HGW has Layer 3 functions (such as PPPoE dialup and NAT), which enable multiple PCs of a family to access the Internet at the same time.
- The STB connected to the HGW provides IPTV program preview and access functions.
- The IAD embedded in the HGW provides one or several POTS ports, which enable multiple phones of a family to access the Internet at the same time.

ONUs applicable to this scenario: MA5616, MA5821, MA5822, MA5622A, MA5623, MA5623A, MA5611S-AE16, MA5611S-AE16 (No SPL), MA5611S-DE16, MA5611S-DE48 (900-ohm impedance), MA5611S-DE48, MA5611S-DE48-A, MA5603T, MA5612, MA5612A. Among these ONUs,

- ONUs with LAN ports include MA5616, MA5821, MA5612, MA5612A.
- ONUs with ADSL2+ ports include MA5616, MA5603T.
- ONUs with VDSL2 ports include MA5616, MA5622A, MA5623, MA5623A, MA5611S-AE16, MA5611S-AE16 (No SPL), MA5611S-DE16, MA5611S-DE48 (900-ohm impedance), MA5611S-DE48, MA5611S-DE48-A, MA5603T.

Figure 11-9 GPON FTTB+HGW Networking for the Internet, VoIP, and IPTV Services (HGW Providing the VoIP Service)

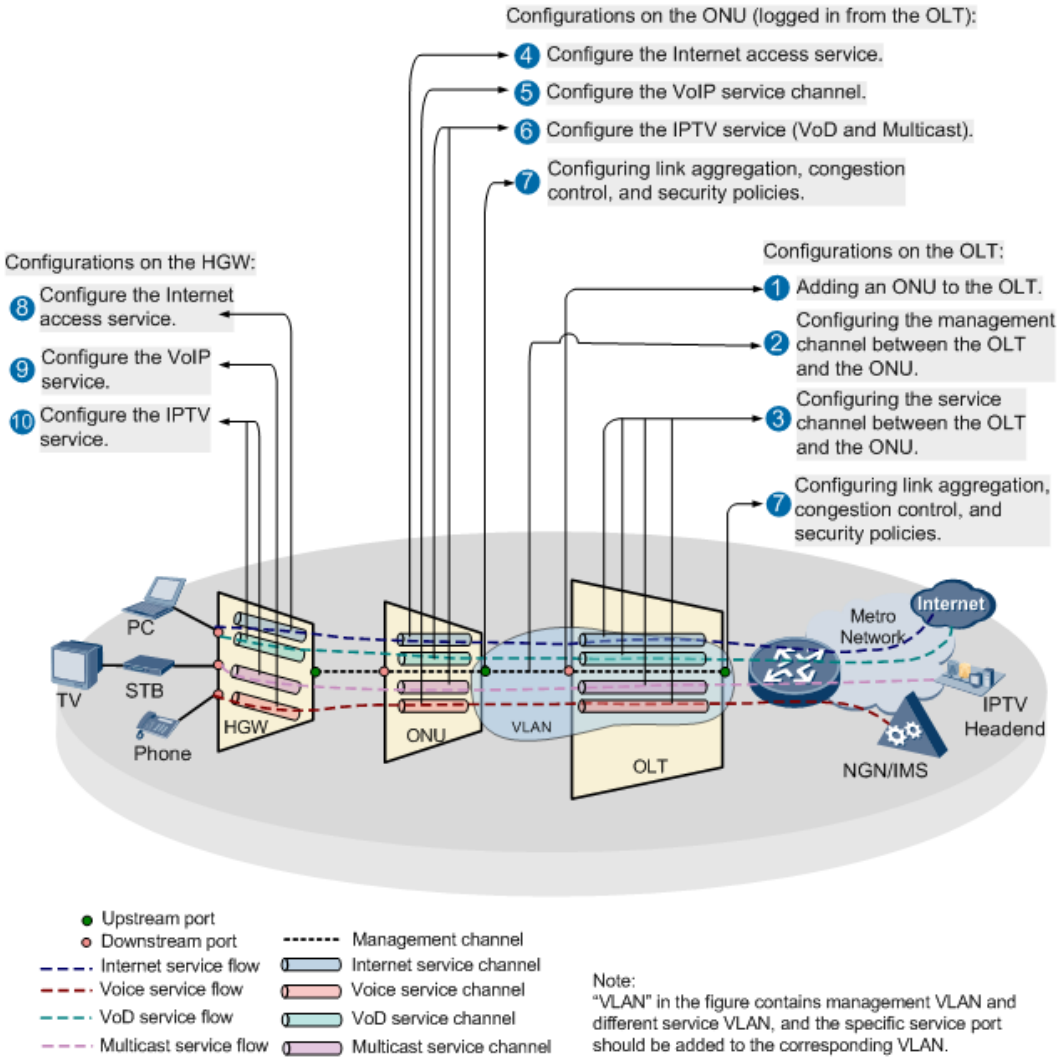


11.3.4.2 Configuration Procedure

Figure 11-10 shows the configuration roadmap diagram in the FTTB+HGW networking scenarios (HGW providing the VoIP service).

Copyright © Huawei Technologies Co., Ltd.

Figure 11-10 Configuration Roadmap Diagram in the FTTB+HGW Networking Scenarios (HGW providing the VoIP service)



The following table describes the configuration procedure.

Configured Device	Procedure	Configuration
OLT	**Add an ONU on the OLT.**	Services can be configured for an ONU only after the ONU is successfully added to an OLT.
	Configure the management channel between the OLT and the ONU.	After the inband management channel between the OLT and the ONU is configured and available, you can log in to the ONU from the OLT to configure the ONU.

Copyright © Huawei Technologies Co., Ltd.

Configured Device	Procedure		Configuration
	Configure the service channel between the OLT and the ONU.	● Configure the Internet access service channel. ● Configure the VoIP service channel. ● Configure the VoD service channel. ● Configure the multicast service channel.	In the FTTB+HGW networking (HGW provides the VoIP service), the ONU provides Internet access service and provides VoIP and IPTV services using the HGW. Therefore, service channels need to be configured on the OLT for different services.
ONU	Configure the Internet access service.	**Configure the LAN Internet access service on the ONU**	**NOTE** Different ONUs have different ports, including LAN, ADSL2+, VDSL2, and VDSL2 vectoring ports, for the Internet access. Select an appropriate configuration method according to the port type.
		Configure the ADSL2+ Internet access service on the ONU.	
		Configure the VDSL2 Internet access service on the ONU.	
		(Optional) Configure vectoring on the ONU	
	Configure the VoIP service channel on the ONU.		In the FTTB+HGW networking (HGW provides the VoIP service), the built-in IAD of the HGW provides the VoIP service. Therefore, VoIP service parameters do not need to be configured on the ONU and only transparent transmission service flows need to be created.

Copyright © Huawei Technologies Co., Ltd.

Configured Device	Procedure		Configuration
	Configure the IPTV service.	● Configure the VoD service. ● Configure the multicast service.	IPTV services include VoD and multicast services that are different in configuration procedures and need to be configured separately.
OLT ONU	**Configure the link aggregation, congestion control, and security policy.**		The global configuration of upstream link aggregation and queue scheduling based on priorities ensures service reliability. The global configuration of security policies ensures service security.
HGW	**Configure the Internet access service on the HGW.**		HGWs have different models and appearances but their configuration procedures are similar. This topic uses the HG239 that uses LAN for upstream transmission and the HG527 uses ADSL2+ for upstream transmission as examples. **NOTE** Vectoring is supported by the HG612 and HG622 only.
	Configure the IPTV services on the HGW.		-
	Configure the VoIP service on the HGW.		This topic describes how to configure the voice service on HGWs that use LAN or xDSL for upstream transmission. This configuration enables home subscribers to enjoy the POTS service by using an analog telephone.
ONU HGW	**Verify the services.**		ONUs provide remote service verification methods including PPPoE dialup emulation, call emulation, and multicast emulation to allow configuration and commissioning engineers to verify services remotely after service configuration. This remote service verification eliminates a second on-site operation. Voice services on the HGW do no support remote service verification.

11.3.4.3 Adding an ONU to an OLT

Services can be configured for an ONU only after the ONU is successfully added to an OLT.

Copyright © Huawei Technologies Co., Ltd.

Context

- When an ONU is added, corresponding profiles need to be bound to the ONU, including the dynamic bandwidth allocation (DBA) profile, line profile, and alarm profile. For details about functions and configuration methods for these profiles, see **Table 11-25**.

Table 11-25 Introduction to ONU profiles

Profile Type	Function	Command
DBA profile	A DBA profile describes GPON traffic parameters. A T-CONT is bound to a DBA profile for dynamic bandwidth allocation, improving upstream bandwidth utilization.	Query a DBA profile. **display dba-profile** Add a DBA profile. **dba-profile add**
Line profile	A line profile describes binding between the T-CONT and the DBA profile, the QoS mode of the service flow, and mapping between the GEM port and the ONU-side service.	Query a line profile. **display ont-lineprofile** Add a line profile. **ont-lineprofile add**
Alarm profile	An alarm profile contains a series of alarm threshold parameters that are used for performance measurement and monitoring of the activated ONT lines.	Query an alarm profile. **display gpon alarm-profile** Add an alarm profile. **gpon alarm-profile add**

- An ONU can be added in two modes. Select either mode as required.

Mode	Usage Scenario	Command
Add an ONU offline.	The ONU password or serial number (SN) is obtained.	Run the **ont add** command to add an ONU.
Online confirm an ONU.	Both the ONU password and SN are not obtained.	In the GPON mode, run the **port ont-auto-find** command to enable the ONU auto-discovery function of a GPON port and then run the **ont confirm** command to add an ONU.

Copyright © Huawei Technologies Co., Ltd.

Data plan

Table 11-26 Data plan

Item	Data
DBA profile	Profile name: fttb_dba Profile type: type3 Assured bandwidth: 8 Mbit/s Maximum bandwidth: 20 Mbit/s
Line profile	Profile name: fttb(c) Profile ID: 10 T-CONT ID: 4 GEM port ID for management service: 11 GEM port ID for Internet access service: 12 GEM port ID for VoIP service: 13
Network topology data	PON port: 0/2/1 ONT ID: 1

Procedure

Step 1 Configure GPON ONU profiles.

1. Configure a DBA profile.

   ```
   huawei(config)#dba-profile add profile-name fttb_dba type3 assure 8192 max 20480
   ```

2. Configure an ONU line profile.

   a. Add GPON ONU line profile 10 fttb(c).

   ```
   huawei(config)#ont-lineprofile gpon profile-id 10 profile-name fttb(c)
   ```

   NOTE

   The ID of the line profile to be created must not exist in the system and the line profile must be created according to the data plan. In this example, line profile 10 is used.

   b. In the line profile mode, bind T-CONT 4 to DBA profile fttb_dba.

   ```
   huawei(config-gpon-lineprofile-10)#tcont 4 dba-profile-name fttb_dba
   ```

   c. In the line profile mode, bind the GEM port to the T-CONT.

   - Add GEM port 11 to carry management service flows.
   - Add GEM port 12 to carry Internet access service flows.
   - Add GEM port 13 to carry VoIP service flows.

   Bind GEM ports 11, 12, and 13 to T-CONT 4. In configuring, QoS policies for various service flows also need to be configured. For details about QoS data plan, see **11.2.2 Principle of QoS Data Plan**.

Copyright © Huawei Technologies Co., Ltd.

```
huawei(config-gpon-lineprofile-10)#gem add 11 eth tcont 4 cascade on
huawei(config-gpon-lineprofile-10)#gem add 12 eth tcont 4 cascade on
huawei(config-gpon-lineprofile-10)#gem add 13 eth tcont 4 cascade on
```

d. Configure mapping between the GEM port and the ONU-side service.

Set the mode for mapping the GEM port to the ONU-side service to the VLAN mapping mode (default). Map management service flows (the CVLAN ID is 8) to GEM port 11, Internet access service flows (the CVLAN ID is 1001) to GEM port 12, and VoIP service flows (the CVLAN ID is 200) to GEM port 13.

```
huawei(config-gpon-lineprofile-10)#gem mapping 11 0 vlan 8
huawei(config-gpon-lineprofile-10)#gem mapping 12 1 vlan 1001
huawei(config-gpon-lineprofile-10)#gem mapping 13 2 vlan 200
```

e. After the configuration is completed, run the **commit** command to make the configured parameters take effect.

```
huawei(config-gpon-lineprofile-10)#commit
huawei(config-gpon-lineprofile-10)#quit
```

3. (Optional) Add an alarm profile.
   - The ID of the default GPON alarm profile is 1. The thresholds for all the alarm parameters in the default alarm profile are 0, which indicates that no alarm is generated.
   - In this example, the default alarm profile is used and therefore the configuration of the alarm profile is not required.

Step 2 Add an ONU to an OLT.

Assume that the ID of GPON port 0/2/1 is 1, SN is 32303131B39FD641, management mode is SNMP, and the bound line profile is fttb(c). Connect the ONU to such a GPON port through the optical splitter.

There are two modes to add an ONT: add an ONT offline and confirm an automatically discovered ONU.

- Add an ONU offline.

```
huawei(config)#interface gpon 0/2
huawei(config-if-gpon-0/2)#ont add 1 ontid 1 sn-auth 32303131B39FD641
snmp ont-lineprofile-name fttb(c)
```

- Confirm an automatically discovered ONU.

```
huawei(config)#interface gpon 0/2
huawei(config-if-gpon-0/2)#port 1 ont-auto-find enable
huawei(config-if-gpon-0/2)#display ont autofind 1
huawei(config-if-gpon-0/2)#ont confirm 1 ontid 1 sn-auth 32303131B39FD641
snmp ont-lineprofile-name fttb(c)
```

1. (Optional) Bind the alarm profile to the ONU.

   By default, alarm profile 1 automatically bound to an ONU. A non-default alarm profile is bound manually only when the default one does not meet the requirement.

   In this example, default alarm profile 1 is used and therefore the configuration of the alarm profile is not required.

Step 3 Check the ONU status.

After an ONU is added, run the **display ont info** command to query the current status of the ONU. Ensure that **Config flag** of the ONU is **active**, **Run State** is **online**, and **Config state** is **normal**.

```
huawei(config-if-gpon-0/2)#display ont info 1 1
  ------------------------------------------------------------------------
  F/S/P                   : 0/2/1
```


Copyright © Huawei Technologies Co., Ltd.

```
  ONT-ID              : 1
  Control flag        : active    //The ONU is activated.
  Run state           : online    //The ONU is online.
  Config state        : normal    //The ONU configurations are recovered
normally.
...//The rest of the response information is not provided here.
huawei(config-if-gpon-0/2)#quit
```

----End

Follow-up Procedure

When **Config state** is **failed**, **Run state** is **offline**, or **Match state** is **mismatch**:

- If **Control flag** is **deactive**, run the **ont active** command in GPON mode to activate the ONU.
- If **Run state** is **offline**, a physical line may be broken or the optical module may be damaged. Check the line and the optical module.
- If **Config state** is **failed**, the configured ONU capability exceeds the actual ONU capability. In this case, run the **display ont failed-configuration** command in the diagnose mode to check the failed configuration item and the failure cause. Then, rectify the fault accordingly.
- If the ONU does not match, that is, **Match state** is **mismatch**, the port types and number of ports undermatch the actual port types and number of ports supported by the ONU. In this case, run the **display ont capability** command to query the actual capability of the ONU, and then select one of the following modes to modify the ONU configuration:
  - Create a proper ONU profile according to the actual capability of the ONU, and then run the **ont modify** command to modify the configuration data of the ONU.
  - Modify the ONU profile according to the actual capability of the ONU and save the modification. Then, the ONU automatically recovers the configuration successfully.

11.3.4.4 Configuring the Management Channel Between the OLT and the ONU

After the inband management channel between the OLT and the ONU is configured and available, you can log in to the ONU from the OLT to configure the ONU.

Data plan

Item	Data	Remarks
Management VLAN and management IP address on the OLT side	Management VLAN ID: 8 Management VLAN type: smart VLAN Inband management IP address: 192.168.50.1/24	To configure the MDU from the OLT by remote logging in to the MDU, the management VLAN of the OLT and that of the MDU must be the same, and the management IP address of the OLT and that of the MDU must be in the same network segment.
Management VLAN and management IP address on the ONU side	Management VLAN ID: 8 Management VLAN type: smart VLAN Inband management IP address: 192.168.50.2/24	

Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Configure the inband management VLAN and IP address of the OLT.

Configure the inband management VLAN to 8, VLAN priority to 6, and the IP address to 192.168.50.1/24.

```
huawei(config)#vlan 8 smart
huawei(config)#port vlan 8 0/19 0
huawei(config)#vlan priority 8 6
huawei(config)#interface vlanif 8
huawei(config-if-vlanif8)#ip address 192.168.50.1 24
huawei(config-if-vlanif8)#quit
```

Step 2 Configure the inband management VLAN and IP address of the ONU.

Configure the static IP address of the ONU to 192.168.50.2/24, gateway to 192.168.50.254, and the management VLAN ID to 8 (the same as the management VLAN of the OLT).

```
huawei(config)#interface gpon 0/2
huawei(config-if-gpon-0/2)#ont ipconfig 1 1 static ip-address 192.168.50.2 mask
255.255.255.0 gateway
192.168.50.254 vlan 8
huawei(config-if-gpon-0/2)#quit
```

Step 3 Configure an inband management service port.

Configure the management service port ID to 1, management VLAN ID to 8, GEM port ID to 11, and user-side VLAN ID to 8. The OLT does not limit inband management service flows. Therefore, it is recommended that you use default traffic profile 6.

```
huawei(config)#service-port 1 vlan 8 gpon 0/2/1 ont 1 gemport 11 multi-service
user-vlan 8 rx-cttr 6 tx-cttr 6
```

Step 4 Confirm that the management channel between the OLT and the ONU is available.

- On the OLT, run the **ping *192.168.50.2*** command to check the connectivity between the OLT and the ONU. The ICMP ECHO-REPLY packet from the ONU should be received.
- On the OLT, you can remote log in to the ONU to perform the configuration.

----End

11.3.4.5 Configuring the Service Channel Between the OLT and the ONU

This topic describes how to configure service channels between an optical line terminal (OLT) and an optical network unit (ONU) on a gigabit-capable passive optical network (GPON). After channels for involved service types are configured on an OLT to which an ONU is connected, packets of the service types from the ONU can be forwarded based on planned VLANs and policies at Layer 2.

Prerequisites

1. **11.3.1.3 Adding an ONU to an OLT** is performed.
2. **11.3.1.4 Configuring the Management Channel Between the OLT and the ONU** is performed.

Copyright © Huawei Technologies Co., Ltd.

Data Plan

The following table provides key information about the service channels between an OLT and an ONU.

Service Type	VLAN Plan	Remarks
Internet access service	S-VLAN ID: 100; S-VLAN attribute: stacking C-VLAN ID: 1000-1016	Plan the Internet access service in per user per service per VLAN (PUPSPV) mode and apply S-VLAN+C-VLAN to differentiate users. For details, see **11.2.3 Principle of Internet Access Service Data Plan**.
VoIP service	S-VLAN ID: 200 C-VLAN ID: 200	The voice over IP (VoIP) service is a carrier-operating, closed service and primarily adopts only S-VLAN tags, which are transparently transmitted by OLTs. For details, see **11.2.5 Principle of VoIP Service Data Plan**.
VoD service	S-VLAN ID: 300	Plan the video on demand (VoD) service in per user per VLAN (PUPV) mode if possible, as the VoD service requires only a few VLAN resources. The VoD service is a carrier-operating, closed service and primarily adopts only S-VLAN tags, which are transparently transmitted by OLTs. For details, see **11.2.6 Principle of IPTV Service Data Plan**.
Multicast service	Multicast VLAN ID: 1000 Multicast cascading port: 0/2/1 IGMP version: IGMPv3 IGMP mode: IGMP proxy Multicast IP address range: 224.1.1.10-224.1.1.100 IP address of the multicast server: 10.10.10.10/24	The multicast service is a carrier-operating, closed service and primarily adopts only S-VLAN tags. For details, see **11.2.6 Principle of IPTV Service Data Plan**.

NOTE

C-VLANs in the preceding table are defined for OLTs. That is, they are upstream VLANs or S-VLANs of ONUs.

Copyright © Huawei Technologies Co., Ltd.

Procedure

- Configure a channel for the Internet access service.
  1. Create an S-VLAN and add an upstream port to it.

     Create S-VLAN 100 with the stacking attribute and add upstream port 0/19/0 to the S-VLAN.

     ```
     huawei(config)#vlan 100 smart
     huawei(config)#vlan attrib 100 stacking
     huawei(config)#port vlan 100 0/19 0
     ```

  2. Configure a traffic profile.

     The 802.1p priority of the Internet access service is 0, and rate limitation is not required. To check whether any existing traffic profile meets the requirements, run the **display traffic table ip** command. In this example, the query result shows that traffic profile 6 meets the requirements, so no traffic profile needs to be configured.

     ```
     huawei(config)#display traffic table ip from-index 0
     ```

  3. Configure a service flow for receiving and transparently transmitting the Internet access service from the ONU side.

     Configure a service flow with the GEM port ID being 12 and user-side VLAN ID being 1001 (example value). The ONU is connected to GPON port 0/2/1, upstream and downstream traffic are rate-limited on the ONU but not on the OLT, and traffic profile 6 is referenced.

     ```
     huawei(config)#service-port vlan 100 gpon 0/2/1 ont 1 gemport 12 multi-
     service user-vlan 1001 tag-transform translate-and-add rx-cttr 6 tx-cttr 6
     ```

- Configure a channel for the VoIP service.
  1. Create an S-VLAN and add an upstream port to it.

     Create S-VLAN 200 with the common attribute and add upstream port 0/19/0 to the S-VLAN.

     ```
     huawei(config)#vlan 200 smart
     huawei(config)#port vlan 200 0/19 0
     ```

  2. Configure a traffic profile.

     The 802.1p priority of the VoIP service is 5, and rate limitation is not required. To check whether any existing traffic profile meets the requirements, run the **display traffic table ip** command. In this example, the query result shows that no traffic profile meets the requirements, so a traffic profile needs to be configured.

     Add traffic profile 9 and set *priority-policy* to **local-setting**. Then, traffic is scheduled based on the priority specified in the traffic profile.

     ```
     huawei(config)#traffic table ip index 9 cir off priority 5 priority-policy
     local-setting
     ```

  3. Configure a service flow for receiving and transparently transmitting the VoIP service from the ONU side.

     Configure a service flow with the GEM port ID being 13 and user-side VLAN ID being 200. The ONU is connected to GPON port 0/2/1, upstream and downstream traffic are rate-limited on the ONU but not on the OLT, and traffic profile 9 is referenced.

Copyright © Huawei Technologies Co., Ltd.

```
huawei(config)#service-port vlan 200 gpon 0/2/1 ont 1 gemport 13 multi-
service user-vlan 200 rx-cttr 9 tx-cttr 9
```

- Configure a channel for the VoD service.
  1. Create an S-VLAN and add an upstream port to it.

     Create S-VLAN 300 with the common attribute and add upstream port 0/19/0 to the S-VLAN.

     ```
     huawei(config)#vlan 300 smart
     huawei(config)#port vlan 300 0/19 0
     ```

  2. Configure a traffic profile.

     The 802.1p priority of the VoD service is 4, and rate limitation is not required. To check whether any existing traffic profile meets the requirements, run the **display traffic table ip** command. In this example, the query result shows that no traffic profile meets the requirements, so a traffic profile needs to be configured.

     Add traffic profile 10 and set *priority-policy* to **local-setting**. Then, traffic is scheduled based on the priority specified in the traffic profile.

     ```
     huawei(config)#traffic table ip index 10 cir off priority 4 priority-
     policy local-Setting
     ```

  3. Configure a service flow for the VoD service.

     Configure a service flow with the GEM port ID being 14 and user-side VLAN ID being 300. The ONU is connected to GPON port 0/2/1, upstream and downstream traffic are rate-limited on the ONU but not on the OLT, and traffic profile 10 is referenced.

     ```
     huawei(config)#service-port vlan 300 gpon 0/2/1 ont 1 gemport 14 multi-
     service user-vlan 300 rx-cttr 10 tx-cttr 10
     ```

- Configure a channel for the multicast service.
  1. Create an S-VLAN and add an upstream port to it.

     Create S-VLAN 1000 with the common attribute and add upstream port 0/19/0 to the S-VLAN.

     ```
     huawei(config)#vlan 1000 smart
     huawei(config)#port vlan 1000 0/19 0
     ```

  2. Configure a service flow for the multicast service.

     Configure a service flow with the GEM port ID being 14 and user-side VLAN ID being 1000. ONT 1 is connected to GPON port 0/2/1, upstream and downstream traffic are rate-limited on the ONU but not on the OLT, and traffic profile 10 is referenced.

     ```
     huawei(config)#service-port vlan 1000 gpon 0/2/1 ont 1 gemport 14 multi-
     service user-vlan 1000 rx-cttr 10 tx-cttr 10
     ```

  3. Configure a multicast cascading port.

     Set GPON port 0/2/1 as a multicast cascading port, ONT ID to 1, and GEM port 14 to carry the multicast service.

     ```
     huawei(config)#btv
     huawei(config-btv)#igmp cascade-port 0/2/1 ontid 1 gemport-index 14
     ```

  4. Set the IGMP version.

     Set the IGMP version to IGMPv3.

Copyright © Huawei Technologies Co., Ltd.

```
huawei(config)#multicast-vlan 1000
huawei(config-mvlan1000)#igmp version v3
```

5. Set the IGMP mode.

   Select the IGMP proxy mode.

   ```
   huawei(config-mvlan1000)#igmp mode proxy
     Are you sure to change IGMP mode?(y/n)[n]:y
   ```

6. Configure an IGMP upstream port.

   Set the IGMP upstream port to port 0/19/0.

   ```
   huawei(config-mvlan1000)#igmp uplink-port 0/19/0
   ```

7. Configure a program library.

   Set the multicast IP address range to 224.1.1.10-224.1.1.100 and the IP address of the multicast server to 10.10.10.10.

   ```
   huawei(config-mvlan1000)#igmp program add batch ip 224.1.1.10 to-ip
   224.1.1.100 sourceip 10.10.10.10
   ```

----End

11.3.4.6 Configuring the Internet Access Service (LAN Access, on the ONU)

This topic describes how to configure the Internet access service for home gateway (HGW) users on an optical network unit (ONU) when HGWs are connected upstream to the ONU through local area networks (LANs).

Data Plan

The following table provides key information about the Internet access service (LAN access).

Item	Data	Remarks
Traffic profile	ID: 8 CIR: 4 Mbit/s VLAN priority: 0 Downstream priority policy: local-setting	-
User VLAN	Untagged	HGWs can send untagged packets or packets with user VLAN tags.
	User VLAN ID: 1, 2, 3...	

Procedure

Step 1 Log in to the ONU to perform the configuration.

You can remote log in to the ONU from the OLT to perform the configuration. User name: **root** (default). Password: **mduadmin** (default).

Step 2 Configure a traffic profile.

Copyright © Huawei Technologies Co., Ltd.

You can run the **display traffic table ip** command to query the traffic profiles existing in the system. If the traffic profiles existing in the system do not meet the requirements, you need to run the **traffic table ip** command to add a traffic profile.

Add traffic profile 8 and set the committed information rate (CIR) to 4 Mbit/s. The priority for upstream packets is 0, and downstream packets are scheduled based on the priority specified in the traffic profile.

```
huawei(config)#traffic table ip index 8 cir 4096 priority 0 priority-policy local-setting
```

Step 3 Create service VLANs.

Create service VLANs 1001-1016 in batches whose type is smart and attribute is common (the service VLAN IDs must be consistent with the user VLAN IDs of the OLT). Add the service VLANs to upstream port 0/0/1.

```
huawei(config)#vlan 1001-1016 smart
huawei(config)#port vlan 1001-1016 0/0 1
```

Step 4 Add a service port.

Configurations for untagged packets and packets with user VLAN tags are different.

- For untagged packets, the configuration is as follows (assuming that the VLAN ID is 1001):

```
   //Create service port 101, bind port 0/3/1 to it, set the user VLAN to untagged, and bind traffic profile 8 to the user VLAN./
huawei(config)#service-port 101 vlan 1001 eth 0/3/1 multi-service user-vlan untagged rx-cttr 8 tx-cttr 8
```

- For packets with user VLAN tags, the configuration is as follows (assuming that the user VLAN ID is 10 and the VLAN ID is 1001):

```
   //Create service port 101, bind port 0/3/1 to it, set the user VLAN ID to 10, and bind traffic profile 8 to the user VLAN./
huawei(config)#service-port 101 vlan 1001 eth 0/3/1 multi-service user-vlan 10 rx-cttr 8 tx-cttr 8
```

----End

11.3.4.7 Configuring the Internet Access Service (ADSL2+ Access, on the ONU)

This topic describes how to configure the Internet access service for home gateway (HGW) users on an optical network unit (ONU) when HGWs are connected upstream to the ONU in ADSL2 + mode.

Context

ADSL2+ ports working in normal mode (that is, RFC 2662 mode) need to bind an ADSL2+ line profile and an ADSL2+ alarm profile. For the functions and configurations of each profile, see **Table 11-27**.

Copyright © Huawei Technologies Co., Ltd.

Table 11-27 ADSL2+ profile

Profile Type	Function	Configuration
ADSL2+ line profile	An ADSL2+ line profile provides the following parameters: ● ADSL/ADSL2+ working mode ● Channel mode ● Upstream/Downstream line rate ● Upstream/Downstream interleave depth ● Noise margin When an ADSL2+ port is activated, the central office (CO) and the customer premises equipment (CPE) negotiate based on the parameters configured in the ADSL2+ line profile, to determine whether the ADSL2+ port can work in the normal state in these conditions.	The system has four default profiles (profile 1, profile 1022, profile 1023, and profile 1024) for activation of ADSL2+ ports in different conditions. ● Profile 1 is used for activation of common ADSL ports. ● Profile 1022 is used for fast activation of ADSL ports. ● Profile 1023 is used for long-reach activation of existing ADSL ports. ● Profile 1024 is used for activation of ports on ADSL2+ boards. Commands: ● To query: **display adsl line-profile** ● To add: **adsl line-profile add** or **adsl line-profile quickadd**
ADSL2+ alarm profile	Values to be configured in an ADSL2 + line alarm profile are thresholds within any 15 minutes. When the statistics of an item reach the threshold, the system informs the device of the event and sends alarms to the NMS.	Commands: ● To query: **display adsl alarm-profile** ● To add: **adsl alarm-profile add** or **adsl alarm-profile quickadd**

Data Plan

The following table provides key information about the Internet access service (ADSL2+ access).

Item	Data	Remarks
Traffic profile	ID: 8 CIR: 4 Mbit/s VLAN priority: 0 Downstream priority policy: local-setting	A traffic profile implements rate-limiting.
VPI/VCI of ADSL2+ users	VPI: 0 VCI: 35	Internet service providers (ISPs) provide VPI/VCI information.

Copyright © Huawei Technologies Co., Ltd.

Item	Data	Remarks
ADSL2+ line profile	ID: 1024 (default); key parameters: ● Working mode: full compatibility ● Channel working mode: interleaved ● Maximum upstream/ downstream rate (kbit/s): 24544/1024	A traffic profile or an ADSL2+ line profile can implement rate-limiting on ADSL2+ ports. This example uses a default traffic profile.
ADSL2+ alarm profile	ID: 1 (default)	The system does not check whether parameter thresholds are crossed and so does not report alarms.

Procedure

Step 1 Log in to the ONU to perform the configuration.

You can remote log in to the ONU from the OLT to perform the configuration. User name: **root** (default). Password: **mduadmin** (default).

Step 2 Configure a traffic profile.

You can run the **display traffic table ip** command to query the traffic profiles existing in the system. If the traffic profiles existing in the system do not meet the requirements, you need to run the **traffic table ip** command to add a traffic profile.

Add traffic profile 8 and set the committed information rate (CIR) to 4 Mbit/s. The priority for upstream packets is 0, and downstream packets are scheduled based on the priority specified in the traffic profile.

```
huawei(config)#traffic table ip index 8 cir 4096 priority 0 priority-policy local-setting
```

Step 3 Create service VLANs.

Create service VLANs 1001-1016 in batches whose type is smart and attribute is common (the service VLAN IDs must be consistent with the user VLAN IDs of the OLT). Add the service VLANs to upstream port 0/0/1.

```
huawei(config)#vlan 1001-1016 smart
huawei(config)#port vlan 1001-1016 0/0 1
```

Step 4 Add a service port.

Assume that the VPI/VCI of users is 0/35 and the VLAN ID is 1001. Add a service port as follows:

```
   //Create service port 101, bind port 0/2/0 to it, set VPI/VCI to 0/35, and bind traffic profile 8 to the user VLAN./
huawei(config)#service-port 101 vlan 1001 adsl 0/2/0 vpi 0 vci 35 multi-service user-vlan untagged rx-cttr 8 tx-cttr 8
```

Step 5 (Optional) Configure an ADSL2+ line profile.

- Configure an ADSL2+ line profile only when the default one does not meet requirements.

Copyright © Huawei Technologies Co., Ltd.

- This example uses the default ADSL2+ line profile (ID: 1024).

Step 6 (Optional) Configure an ADSL2+ alarm profile.

This example uses the default ADSL2+ alarm profile (ID: 1).

Step 7 Bind an ADSL2+ line profile and an ADSL2+ alarm profile, and activate the ADSL2+ port.

For example, bind ADSL2+ line profile 1024 and ADSL2+ alarm profile 1, and activate ADSL2+ port 0/2/0.

```
huawei(config)#interface adsl 0/2
huawei(config-if-adsl-0/2)#deactivate 0
huawei(config-if-adsl-0/2)#alarm-config 0 1
huawei(config-if-adsl-0/2)#activate 0 profile-index 1024
```

----End

11.3.4.8 Configuring the Internet Access Service (VDSL2 Access, on the ONU)

This topic describes how to configure the Internet access service for home gateway (HGW) users on an optical network unit (ONU) when HGWs are connected upstream to the ONU in VDSL2 mode.

Context

VDSL2 ports working in normal mode (that is, TR129 mode) need to bind the VDSL2 line template and VDSL2 alarm template. For the functions and configurations of each profile, see **Table 11-28**.

Table 11-28 VDSL2 template

Template Type	Function	Configuration
VDSL2 line template	A VDSL2 line template consists of a VDSL2 line profile and a VDSL2 channel profile. When a VDSL2 port is activated, the central office (CO) and the customer premises equipment (CPE) negotiate based on the parameters configured in the VDSL2 line template, to determine whether the VDSL2 port can work in the normal state in these conditions.	The system has one default VDSL2 line template (template 1), which is used for activation of common VDSL2 ports. ● To query: **display vdsl line-template** ● To add: **vdsl line-template add** or **vdsl line-template quickadd**
	A VDSL2 line profile provides the following parameters: line transmission mode, adaptation mode of upstream/downstream transmit rates, signal-to-noise ratio (SNR) margin, upstream power back-off (UPBO), and downstream power back-off (DPBO).	● To query: **display vdsl line-profile** ● To add: **vdsl line-profile add** or **vdsl line-profile quickadd**

Copyright © Huawei Technologies Co., Ltd.

Template Type	Function	Configuration
	A VDSL2 channel profile provides the following parameters: data channel mode, minimum impulse noise protection, interleaved delay parameters, rate parameters, retransmission at the physical layer, erasure decoding, and G.998.4 retransmission.	● To query: **display vdsl channel-template** ● To add: **vdsl channel-template add** or **vdsl channel-profile quickadd**
VDSL2 alarm template	A VDSL2 alarm template consists of a VDSL2 line alarm profile and a VDSL2 channel alarm profile. Values to be configured in a VDSL2 alarm template are thresholds within any 15 minutes. When the statistics of an item reach the threshold, the system informs the device of the event, and sends alarms to the NMS.	The system has one default VDSL2 alarm template (template 1). ● To query: **display vdsl alarm-template** ● To add: **vdsl alarm-template add** or **vdsl alarm-template quickadd**
	A VDSL2 line alarm profile provides the following parameters for COs and CPEs: ● Forward error check seconds (FECS) ● Errored seconds (ES) ● Severely errored seconds (SES) ● Loss of signal seconds (LOSS) ● Unavailable seconds (UAS) ● Low error-free throughput rate (LEFTR) defect seconds	● To query: **display vdsl alarm-profile** ● To add: **vdsl alarm-profile add** or **vdsl alarm-profile quickadd**
	A VDSL2 channel alarm profile provides the following parameters for COs and CPEs: ● Coding violations counts (CVC) ● Corrected blocks counts (CBC)	● To query: **display vdsl channel-alarm-profile** ● To add: **vdsl channel-alarm-profile add** or **vdsl channel-alarm-profile quickadd**

Data Plan

Table 11-29 provides key information about the Internet access service (VDSL2 access).

Copyright © Huawei Technologies Co., Ltd.

Table 11-29 Key information about the Internet access service (VDSL2 access)

Item	Data	Remarks
Traffic profile	ID: 8 CIR: 4 Mbit/s VLAN priority: 0 Downstream priority policy: local-setting	A traffic profile implements rate-limiting.
VDSL2 line mode	PTM	There are two VDSL line modes: ATM mode and PTM mode. ● ATM mode: ATM cells are transmitted in channels. This mode is compatible with the ADSL2+ mode. ● PTM mode: IP cells are transmitted in channels. This mode is incompatible with the ADSL2+ mode. This example assumes the PTM mode.
VDSL2 line template	Line profile ID: 1 (default)	A traffic profile or a VDSL2 line template can implement rate-limiting on VDSL2 ports. This example uses a default traffic profile.
	Channel profile ID: 1 (default)	
	Line template ID: 1 (default)	
VDSL2 alarm template	Line alarm profile ID: 1 (default)	The system does not check whether parameter thresholds are crossed and so does not report alarms.
	Channel alarm profile ID: 1 (default)	
	Alarm template ID: 1 (default)	

Procedure

Step 1 Log in to the ONU to perform the configuration.

You can remote log in to the ONU from the OLT to perform the configuration. User name: **root** (default). Password: **mduadmin** (default).

Step 2 Configure a traffic profile.

You can run the **display traffic table ip** command to query the traffic profiles existing in the system. If the traffic profiles existing in the system do not meet the requirements, you need to run the **traffic table ip** command to add a traffic profile.

Add traffic profile 8 and set the committed information rate (CIR) to 4 Mbit/s. The priority for upstream packets is 0, and downstream packets are scheduled based on the priority specified in the traffic profile.

Copyright © Huawei Technologies Co., Ltd.

```
huawei(config)#traffic table ip index 8 cir 4096 priority 0 priority-policy local-setting
```

Step 3 Create service VLANs.

Create service VLANs 1001-1016 in batches whose type is smart and attribute is common (the service VLAN IDs must be consistent with the user VLAN IDs of the OLT). Add the service VLANs to upstream port 0/0/1.

```
huawei(config)#vlan 1001-1016 smart
huawei(config)#port vlan 1001-1016 0/0 1
```

Step 4 Add a service port.

Assume that the VDSL2 path mode is PTM mode, VLAN ID is 1001, port is 0/1/0, packets from the user VLAN are untagged, and service flow ID is 101. Add a service port as follows:

```
huawei(config)#service-port 101 vlan 1001 vdsl mode ptm 0/1/0 multi-service user-vlan untagged rx-cttr 8 tx-cttr 8
```

Step 5 Configure a VDSL2 line template.

This example uses the default VDSL2 line template (ID: 1).

Step 6 Configure a VDSL2 alarm template.

This example uses the default VDSL2 alarm template (ID: 1).

Step 7 Bind a VDSL2 line template and a VDSL2 alarm template, and activate the VDSL2 port.

For example, bind VDSL2 line template 1 and VDSL2 alarm template 1, and activate VDSL2 port 0/1/0.

```
huawei(config)#interface vdsl 0/1
huawei(config-if-vdsl-0/1)#deactivate 0
huawei(config-if-vdsl-0/1)#alarm-config 0 1
huawei(config-if-vdsl-0/1)#activate 0 template-index 1
```

----End

11.3.4.9 (Optional) Configuring Vectoring

Vectoring configurations on VDSL2 lines cancel the far-end crosstalk (FEXT) of VDSL2 lines to improve the line rate.

Context

For MA5623A/MA5616, when configuring vectoring, learn configuration item functions and configuration methods beforehand by referring to **Table 11-30**.

Copyright © Huawei Technologies Co., Ltd.

Table 11-30 Vectoring configuration items

Item	Function	Description	Commands
Global band plan	In the vectoring algorithm, the system requires that the upstream band and downstream band are separate from each other. Therefore, the band plan must be globally configured.	● The band plan can be globally configured only when vectoring is globally enabled. ● After vectoring is globally enabled, if the band plan configured for the line profile is incompatible with the band plan globally configured for vectoring and the upstream band plan and downstream band plan are not separate from each other, the port cannot be activated.	xdsl vectoring bandplan-type
Global vectoring configurations	Vectoring configurations take effect only when vectoring is globally enabled.	● Before enabling vectoring, globally configure the band plan. **NOTE** Services in a vectoring group port are interrupted when the vectoring function is enabled or disabled.	xdsl vectoring

Copyright © Huawei Technologies Co., Ltd.

Item	Function	Description	Commands
Vectoring profile	Configure the function of canceling the upstream and downstream crosstalk in the vectoring profile. After binding the configured vectoring profile to the ports, the system implements the vectoring algorithm on the ports in the vectoring group based on profile configurations.	By default, all ports are bound to vectoring profile 1. Default value: ● Upstream crosstalk cancelation: enable ● Downstream crosstalk cancelation: enable	Query a vectoring profile: display xdsl vectoring-profile
Policy for controlling frequent online and offline on ports	The Vectoring algorithm is executed every time a port in a Vectoring group goes online or offline. To prevent adverse impact on system functions due to long-term running Vectoring tasks caused by frequent online and offline on a port, set the policy for controlling frequent online and offline on ports based on site requirements.	By default, the policy for controlling frequent online and offline is set to limit.	xdsl frequently-retrain-control
Vectoring crosstalk matrix	The vectoring crosstalk matrix refers to crosstalk on a port in a vectoring group from other ports in the same vectoring group.	Before querying information about the vectoring crosstalk matrix, ensure that the global vectoring function is enabled and the specified port is in a vectoring group and activated.	display xdsl vectoring crosstalk-coupling-matrix

Copyright © Huawei Technologies Co., Ltd.

Item	Function	Description	Commands
Policy for activating a legacy customer premises equipment (CPE)	A legacy CPE is a VDSL2 CPE (supporting G.993.2, not G.993.5) that does not support Vectoring. If such a CPE is activated in G.993.2 mode in the Vectoring system, the crosstalk impact on other lines cannot be canceled, causing the Vectoring system performance to deteriorate. To minimize the impact, set the activation policy of a legacy CPE based on site requirements.	By default, the policy for activating a legacy CPE is set to limit. ● **no-limit**: The Vectoring legacy CPE is activated in common VDSL2 mode (G.993.2 mode), or non-Vectoring mode, in which the Vectoring system performance is affected. This mode is used in the Vectoring initial phase when a large number of CPEs need to be upgraded or replaced and the Vectoring performance are not concerned. ● **limit**: The Vectoring legacy CPE is activated in common VDSL2 mode but the line PSD is automatically shaped so that the CPE can be activated at a low VDSL2 rate, preventing crosstalk on other lines. This mode is used in Vectoring medium phase when some CPEs have not been upgrade or replaced. ● **force-friendly-ds-limit-us**: **force friendly** is used in the downstream	xdsl vectoring legacy-cpe activate-policy

Copyright © Huawei Technologies Co., Ltd.

Item	Function	Description	Commands
		direction and PSD automatic shaping is used in the upstream direction. ● **force-friendly-ds-no-limit-us**: **force friendly** is used in the downstream direction and no restriction is used in the upstream direction. ● **block**: The Vectoring legacy CPE cannot be activated in common VDSL2 mode. This mode is used in Vectoring mature phase when its performance is concerned and unnecessary crosstalk must be prevented.	

For MA5603T, when configuring vectoring, learn configuration item functions and configuration methods beforehand by referring to **Table 11-31**.

Copyright © Huawei Technologies Co., Ltd.

Table 11-31 Vectoring configuration items

Item	Function	Description	Commands
Global band plan	In the vectoring algorithm, the system requires that the upstream band and downstream band are separate from each other. Therefore, the band plan must be globally configured.	● The band plan can be globally configured only when vectoring is globally enabled. ● After vectoring is globally enabled, if the band plan configured for the line profile is incompatible with the band plan globally configured for vectoring and the upstream band plan and downstream band plan are not separate from each other, the port cannot be activated.	xdsl vectoring bandplan-type
Global vectoring configurations	Vectoring configurations take effect only when vectoring is globally enabled.	● Vectoring can be globally enabled only when devices are configured with VP boards. ● Before enabling vectoring, globally configure the band plan. **NOTE** Services in a vectoring group port are interrupted when the vectoring function is enabled or disabled.	xdsl vectoring

Copyright © Huawei Technologies Co., Ltd.

Item	Function	Description	Commands
Vectoring profile	Configure the function of canceling the upstream and downstream crosstalk in the vectoring profile. After binding the configured vectoring profile to the ports, the system implements the vectoring algorithm on the ports in the vectoring group based on profile configurations.	By default, all ports are bound to vectoring profile 1. Default value: ● Upstream crosstalk cancelation: enable ● Downstream crosstalk cancelation: enable	Commands: ● Add a vectoring profile: xdsl vectoring-profile add ● Modify a vectoring profile: xdsl vectoring-profile modify ● Delete a vectoring profile: xdsl vectoring-profile delete ● Query a vectoring profile: display xdsl vectoring-profile ● Bind a vectoring profile to the port: vectoring-config (VDSL mode)
Policy for controlling frequent online and offline on ports	The Vectoring algorithm is executed every time a port in a Vectoring group goes online or offline. To prevent adverse impact on system functions due to long-term running Vectoring tasks caused by frequent online and offline on a port, set the policy for controlling frequent online and offline on ports based on site requirements.	By default, the policy for controlling frequent online and offline is set to limit.	xdsl frequently-retrain-control

Copyright © Huawei Technologies Co., Ltd.

Item	Function	Description	Commands
Vectoring crosstalk matrix	The vectoring crosstalk matrix refers to crosstalk on a port in a vectoring group from other ports in the same vectoring group.	Before querying information about the vectoring crosstalk matrix, ensure that the global vectoring function is enabled and the specified port is in a vectoring group and activated.	display xdsl vectoring crosstalk-coupling-matrix

Copyright © Huawei Technologies Co., Ltd.

Item	Function	Description	Commands
Policy for activating a legacy customer premises equipment (CPE)	A legacy CPE is a VDSL2 CPE (supporting G. 993.2, not G. 993.5) that does not support Vectoring. If such a CPE is activated in G.993.2 mode in the Vectoring system, the crosstalk impact on other lines cannot be canceled, causing the Vectoring system performance to deteriorate. To minimize the impact, set the activation policy of a legacy CPE based on site requirements.	By default, the policy for activating a legacy CPE is set to limit. ● **no-limit**: The Vectoring legacy CPE is activated in common VDSL2 mode (G.993.2 mode), or non-Vectoring mode, in which the Vectoring system performance is affected. This mode is used in the Vectoring initial phase when a large number of CPEs need to be upgraded or replaced and the Vectoring performance are not concerned. ● **limit**: The Vectoring legacy CPE is activated in common VDSL2 mode but the line PSD is automatically shaped so that the CPE can be activated at a low VDSL2 rate, preventing crosstalk on other lines. This mode is used in Vectoring medium phase when some CPEs have not been upgrade or replaced. ● **force-friendly-ds-limit-us**: **force friendly** is used in the downstream	xdsl vectoring legacy-cpe activate-policy

Copyright © Huawei Technologies Co., Ltd.

Item	Function	Description	Commands
		direction and PSD automatic shaping is used in the upstream direction. ● **force-friendly-ds-no-limit-us**: **force friendly** is used in the downstream direction and no restriction is used in the upstream direction. ● **block**: The Vectoring legacy CPE cannot be activated in common VDSL2 mode. This mode is used in Vectoring mature phase when its performance is concerned and unnecessary crosstalk must be prevented.	

Data Plan

The **Table 11-32** lists key parameters of vectoring configurations.

Table 11-32 Key parameters of vectoring configurations

Item	Data	Description
Global vectoring configurations	enable	-
Global band plan	● Band plan type: 998ade ● USO type: type-a	-
Policy for activating a legacy customer premises equipment (CPE)	no-limit	The policy for activating a vectoring legacy CPE is configured as **no-limit** at the initial stage of vectoring application.

Copyright © Huawei Technologies Co., Ltd.

Item	Data	Description
Policy for controlling frequent online and offline on ports	no-limit	-
Vectoring group	Group ID: 1	All ports are added to the default vectoring group 1.
Vectoring profile	For the MA5623A/MA5616: Profile ID: 1 The upstream/ downstream crosstalk cancelation function in default Profile 1 are as follows: ● Upstream crosstalk cancelation: enable ● Downstream crosstalk cancelation: enable	-
	For MA5603T: ● Profile name: huawei ● Upstream crosstalk cancelation: enable ● Downstream crosstalk cancelation: enable ● The port to which a vectoring profile is bound: all ports on the0/1 board.	

NOTE

The Vectoring is configured on the ONU, and the configuration between the MA5623A/MA5616 and MA5603T is a little different, Here gives the configuring steps of MA5623A/MA5616 and MA5603T respectively.

Procedure

- Configuration procedure for the MA5623A/MA5616:
  1. Log in to the ONU remotely and start the configuration.

     By default, the user name is **root** and the password is **mduadmin**.
  2. Globally configure the band plan type.

     ```
     huawei(config)#xdsl vectoring bandplan-type 998ade us0-type type-a
     ```
  3. Configure the policy for activating a vectoring legacy CPE.

     ```
     huawei(config)#xdsl vectoring legacy-cpe activate-policy no-limit
     ```
  4. Configure the policy for controlling frequent online and offline on ports.

     ```
     huawei(config)#xdsl frequent-retrain-control 0/1/0 control-policy no-limit
     ```
  5. Enable global vectoring.

Copyright © Huawei Technologies Co., Ltd.

```
huawei(config)#xdsl vectoring enable
```

6. Save the data.

```
huawei(config)#save
```

- Configuration procedure for the MA5603T:

1. Log in to the ONU remotely and start the configuration.

   By default, the user name is **root** and the password is **admin**.

2. Globally configure the band plan type.

```
huawei(config)#xdsl vectoring bandplan-type 998ade us0-type type-a
```

3. Configure the vectoring profile as **huawei** and bind it to the VDSL2 port in the vectoring group.

```
huawei(config)#xdsl vectoring-profile add control enable enable name
huawei
huawei(config)#interface vdsl 0/1
huawei(config-if-vdsl-0/1)#vectoring-config all profile-name huawei
huawei(config-if-vdsl-0/1)#quit
```

4. Configure the policy for activating a vectoring legacy CPE.

```
huawei(config)#xdsl vectoring legacy-cpe activate-policy no-limit
```

5. Configure the policy for controlling frequent online and offline on ports.

```
huawei(config)#xdsl frequent-retrain-control 0/1/0 control-policy no-limit
```

6. Enable the global vectoring.

```
huawei(config)#xdsl vectoring enable
```

7. Save the data.

```
huawei(config)#save
```

----End

11.3.4.10 Configuring the Voice Service Channel (on the ONU)

This topic describes how to configure the VoIP service on an ONU. In this scenario, The HGW provides the VoIP service and the ONU is configured to establish VoIP service channels.

Data Plan

Data plan for configuring the VoIP service on the ONU

Item	Data	Remarks
Upstream VLAN	200	The upstream VLAN on the ONU is also called the SVLAN on the ONU. It corresponds to the CVLAN on the OLT. The VoIP service is a closed service operated by carriers. SVLAN with a single tag is the mainstream application. The OLT transparently transmits the SVLAN of the ONU.

Copyright © Huawei Technologies Co., Ltd.

Item	Data	Remarks
Traffic profile	ID: 9 Committed rate: off VLAN priority Priority policy: Local-Setting	For the VoIP service, it is recommended to rate limit traffic on the BRAS or SR without using traffic profiles.
User port	The HGW uses LAN for upstream transmission: The HGW uses ADSL2+ for upstream transmission: The HGW uses VDSL2 for upstream transmission:	Different types of HGWs establish service flows in different ways.
User VLAN on the HGW	200	It is recommended that the user VLAN on the HGW be the same as the upstream VLAN on the ONU when the HGW provides the VoIP service.

Procedure

Step 1 Create the upstream VLAN and add upstream ports 0/0/1 to it.

```
huawei(config)#vlan 200 smart
huawei(config)#port vlan 200 0/0 1
```

Step 2 Configure a VoIP service traffic profile.

The 802.1p priority of the VoIP service is 5 and the traffic profile specifies no rate limit. Run the **display traffic table ip** command to query existing traffic profiles in the system. If there is no traffic profile to meet the requirements listed in the data plan, create one.

Add traffic profile 9 and set **Local-Setting** to *priority-policy* so that packets are scheduled according to their priorities.

```
huawei(config)#traffic table ip index 9 cir off priority 5 priority-policy Local-
Setting
```

Step 3 Create the VoIP service flow.

- For the HGW that uses LAN for upstream transmission, the VoIP service is configured as follows:
  ```
  huawei(config)#service-port 201 vlan 200 eth 0/3/1 multi-service user-vlan
  200 rx-cttr 9 tx-cttr 9
  ```
- For the HGW that uses ADSL2+ for upstream transmission, the VoIP service is configured as follows:
  ```
  huawei(config)#service-port 201 vlan 200 adsl 0/2/0 vpi 0 vci 35 multi-service
  user-vlan
  200 rx-cttr 9 tx-cttr 9
  ```
- For the HGW that uses VDSL2 for upstream transmission, the VoIP service is configured as follows:

Copyright © Huawei Technologies Co., Ltd.

```
huawei(config)#service-port 201 vlan 200 vdsl mode ptm 0/1/0 multi-service
user-vlan
200 rx-cttr 9 tx-cttr 9
```

----End

11.3.4.11 Configuring the IPTV Service (on the ONU)

This topic describes how to configure the video on demand (VoD) service and multicast service for home gateway (HGW) users on an optical network unit (ONU) when HGWs are connected upstream to the ONU through local area networks (LANs) or in xDSL mode.

Data Plan

The following table provides key information about the IPTV service.

Item	Data	Remarks
Traffic profile	ID: 10 CIR: off VLAN priority: 4 Downstream priority policy: local-setting	-
User VLAN in the scenario in which HGWs are upstream connected to an ONU through LANs	User VLAN ID: 1, 2, 3...	HGWs can send untagged packets or packets with user VLAN tags.
VPI/VCI of ADSL2+ users in the scenario in which HGWs are connected upstream to an ONU in ADSL2+ mode	VPI: 0 VCI: 35	Internet service providers (ISPs) provide VPI/VCI information.

Copyright © Huawei Technologies Co., Ltd.

Item	Data	Remarks
VDSL2 path mode in the scenario in which HGWs are connected upstream to an ONU in VDSL2 mode	PTM	Both the central office and HGWs must support the PTM mode.
VLAN ID of the VoD service	300	The VoD service is a carrier-operating, closed service and primarily adopts only SVLAN tags, which are transparently transmitted by OLTs.
Multicast VLAN ID of the ONU	1000	-
Multicast VLAN ID of HGWs	43	A carrier generally specifies a globally unique multicast VLAN ID for HGWs.

Procedure

- Configure the VoD service.

  Create VLAN 300 with the common attribute and add upstream port 0/0/1 to the VLAN.

  ```
  huawei(config)#vlan 300 smart
  huawei(config)#port vlan 300 0/0 1
  ```

  Configure a traffic profile for the IPTV service.

  The IEEE 802.1p priority of the IPTV service is 4, and rate limitation is not required. To check whether any existing traffic profile meets the requirements, run the **display traffic table ip** command. In this example, the query result shows that no traffic profile meets the requirements, so a traffic profile needs to be configured.

  Add traffic profile 10 and set *priority-policy* to **local-setting**. Then, traffic is scheduled based on the priority specified in the traffic profile.

  ```
  huawei(config)#traffic table ip index 10 cir off priority 4 priority-policy
  local-setting
  ```

  Configure a service flow for the VoD service.

  Configurations vary according to upstream interface types of HGWs.

  - If HGWs are connected to an ONU upstream through LANs and upstream packets contain user VLAN tags, the ONU needs to perform a switch between user VLAN IDs and SVLAN IDs.

Copyright © Huawei Technologies Co., Ltd.

Assume that the user VLAN ID is 1 and the Ethernet port is 0/3/1. Add a service flow as follows:

```
huawei(config)#service-port 301 vlan 300 eth 0/3/1 multi-service user-vlan
1 rx-cttr 10 tx-cttr 10
```

- If HGWs are connected to an ONU upstream in ADSL2+ mode, upstream packets contain users' PVC information so the ONU needs to perform a switch between PVC information and SVLAN IDs.

  Assume that the VPI/VCI is 0/35 and the ADSL2+ port is 0/2/0. Add a service flow as follows:

  ```
  huawei(config)#service-port 301 vlan 300 adsl vpi 0 vci 35 0/2/0 multi-
  service user-vlan untagged rx-cttr 10 tx-cttr 10
  ```

- If HGWs are connected to an ONU upstream in VDSL2 mode, formats of upstream packets depend on the encapsulation mode.

  Assume that the VDSL2 path mode is PTM mode, port is 0/1/0, and packets from the user VLAN are untagged. Add a service flow as follows:

  ```
  huawei(config)#service-port 301 vlan 300 vdsl mode ptm 0/1/0 multi-service
  user-vlan untagged rx-cttr 10 tx-cttr 10
  ```

- Configure the multicast service.

  Create multicast VLAN 1000 with the common attribute and add upstream port 0/0/1 to the multicast VLAN.

  ```
  huawei(config)#vlan 1000 smart
  huawei(config)#port vlan 1000 0/0 1
  ```

  Set the IGMP version to IGMP v3.

  ```
  huawei(config)#multicast-vlan 1000
  huawei(config-mvlan1000)#igmp version v3
  ```

  Set the IGMP mode to IGMP proxy.

  ```
  huawei(config-mvlan1000)#igmp mode proxy
    Are you sure to change IGMP mode?(y/n)[n]:y
  ```

  Configure an IGMP upstream port.

  ```
  huawei(config-mvlan1000)#igmp uplink-port 0/0/1
  ```

  Configure a program library. Set the multicast IP address range to 224.1.1.10-224.1.1.100 and the IP address of the multicast server to 10.10.10.10.

  ```
  huawei(config-mvlan1000)#igmp program add batch ip 224.1.1.10 to-ip
  224.1.1.100 sourceip 10.10.10.10
  huawei(config-mvlan1000)#quit
  ```

  Configure a service flow for the multicast service.

  Configurations vary according to upstream interface types of HGWs.

  - If HGWs are connected to an ONU upstream through LANs, assume that the user VLAN ID is 43 and the Ethernet port is 0/3/1, and add a service flow as follows:
    ```
    huawei(config)#service-port 401 vlan 1000 eth 0/3/1 multi-service user-vlan
    43 rx-cttr 10 tx-cttr 10
    ```
  - If HGWs are connected to an ONU upstream in ADSL2+ mode, assume that the VPI/VCI is 0/35 and the ADSL2+ port is 0/2/0, and add a service flow as follows:
    ```
    huawei(config)#service-port 401 vlan 1000 adsl vpi 0 vci 35 0/2/0 multi-
    service user-vlan untagged rx-cttr 10 tx-cttr 10
    ```


Copyright © Huawei Technologies Co., Ltd.

- If HGWs are connected to an ONU upstream in VDSL2 mode, assume that the VDSL2 path mode is PTM mode, the user VLAN ID is 43, and the VDSL2 port is 0/1/0, and add a service flow as follows:

```
huawei(config)#service-port 401 vlan 1000 vdsl mode ptm 0/1/0 multi-service user-vlan 43 rx-cttr 10 tx-cttr 10
```

Configure a multicast user and add the user to the multicast VLAN.

Configure service flow 401 as a multicast user, add the user to multicast VLAN 1000, and adopt the no-auth mode for the multicast user.

```
huawei(config-mvlan1000)#btv
huawei(config-btv)#igmp user add service-port 401 no-auth
huawei(config-btv)#multicast-vlan 1000
huawei(config-mvlan1000)#igmp multicast-vlan member service-port 401
huawei(config-mvlan1000)#quit
```

----End

11.3.4.12 Configuring Link Aggregation, Congestion Control, and Security Policy

The global configuration of upstream link aggregation and queue scheduling based on priorities ensures service reliability. The global configuration of security policies ensures service security.

Context

Link aggregation provides a higher bandwidth and uplink reliability for optical line terminals (OLTs) by aggregating multiple uplink Ethernet ports to one link aggregation group (LAG). Link aggregation is recommended.

Congestion control places the packets to be sent from a port into multiple queues that are marked with different priorities. Then, the packets are sent based on queue priorities. Congestion control is recommended.

Security policies ensure system, user, and service security.

NOTE

Enable a service security function based on the service type. For details, see **11.2.7 Principle of Security Data Plan**.

Procedure

- Configure link aggregation.

  The following configurations are used as an example to configure link aggregation:

  - Uplink ports 0/19/0 and 0/19/1 are added to a LAG.
  - The two ports send packets upstream based on the packets' source MAC addresses.
  - The LAG works in Link Aggregation Control Protocol (LACP) static aggregation mode.

```
huawei(config)#link-aggregation 0/19 0-1 ingress workmode lacp-static
```

- Configure queue scheduling.

  According to quality of service (QoS) planning principles, all packets are scheduled in strict priority (SP) mode and mapped to queues according to the packets' priorities. For details about QoS planning principles, see **11.2.2 Principle of QoS Data Plan**.

```
huawei(config)#queue-scheduler strict-priority
huawei(config)#cos-queue-map cos0 0 cos4 4 cos5 5 cos6 6
```


Copyright © Huawei Technologies Co., Ltd.

- Configure system security.
  - Enable deny of service (DoS) anti-attack on both the OLT and optical network units (ONUs).
    1. Run the **security anti-dos enable** command to globally enable DoS anti-attack.
    2. Run the **security anti-dos control-packet policy** command to configure a protocol packet processing policy that will be used when a DoS attack occurs.
    3. Run the **security anti-dos control-packet rate** command to configure the threshold for the rate of sending protocol packets to the CPU.
  - Enable IP address anti-attack on both the OLT and ONUs.

    Run the **security anti-ipattack enable** command to enable IP address anti-attack.
- Configure user security.
  - Enable MAC address anti-flapping on both the OLT and ONUs.

    Run the **security anti-macduplicate enable** command to enable MAC address anti-flapping.
  - Enable MAC address anti-spoofing on both the OLT and ONUs.
    1. In global config mode, run the **security anti-macspoofing enable** command to globally enable MAC address anti-spoofing.
    2. Enable MAC address anti-spoofing at VLAN level in global config mode or service profile mode:
       a. In global config mode, run the **security anti-macspoofing vlan** command to enable MAC address anti-spoofing.
       b. Perform the following operations to enable MAC address anti-spoofing in service profile mode:
          a. In global config mode, run the **vlan service-profile** command to create a VLAN service profile.
          b. Run the **security anti-macspoofing enable** command to enable MAC address anti-spoofing at VLAN level.
          c. Run the **commit** command to make the profile configuration take effect.
          d. Run the **quit** command to quit the VLAN service profile mode.
          e. Run the **vlan bind service-profile** command to bind the created VLAN service profile to a VLAN.
    3. (Optional) Run the **security anti-macspoofing max-mac-count** command to set the maximum number of MAC addresses that can be bound to a service flow.
    4. (Optional) Run the **security anti-macspoofing exclude** command to configure the types of packets for which MAC address anti-spoofing does not take effect, such as Internet Group Management Protocol (IGMP) packets.
  - Enable IP address anti-spoofing on ONUs.

    IP address anti-spoofing can be enabled or disabled at three levels: global, VLAN, and service port levels. This function takes effect only after it is enabled at the three levels. Among the three levels, IP address anti-spoofing is disabled only at the global level by default.

Copyright © Huawei Technologies Co., Ltd.

1. In global config mode, run the **security anti-ipspoofing enable** command to enable IP address anti-spoofing at the global level.
2. In VLAN service profile mode, run the **security anti-ipspoofing enable** command to enable IP address anti-spoofing at the VLAN level.
3. Run the **security anti-ipspoofing service-port** *serviceport-id* **enable** command to enable IP address anti-spoofing at the service port level.

- Configure service security.
  - Enable Dynamic Host Configuration Protocol (DHCP) Option 82 on both the OLT and ONUs. This configuration is recommended for the DHCP-based Internet access service.

    1. Enable DHCP Option 82 on both the OLT and ONUs.

       DHCP Option 82 can be enabled or disabled at four levels: global, port, VLAN, and service port levels. This function takes effect only after it is enabled at the four levels. Among the four levels, DHCP Option 82 is disabled only at the global level by default.

       - The global level: In global config mode, run the **dhcp option82** command to enable DHCP Option 82 at the global level.

         When you run this command, select the **enable**, **forward**, or **rebuild** parameter based on site requirements. The three parameters can all enable DHCP Option 82 but provide different packet processing policies on the OLT. For details, see the **dhcp option82** command.
       - The port level: In global config mode, run the **dhcp option82 port** or **dhcp option82 board** command to enable DHCP Option 82 at the port level.
       - The VLAN level:

         a. In global config mode, run the **vlan service-profile** command to create a VLAN service profile.

         b. Run the **dhcp option82 enable** command to enable DHCP Option 82 at the VLAN level.

         c. Run the **commit** command to make the profile configuration take effect.

         d. Run the **quit** command to quit the VLAN service profile mode.

         e. Run the **vlan bind service-profile** command to bind the created VLAN service profile to a VLAN.
       - The service port level: In global config mode, run the **dhcp option82 service-port** command to enable DHCP Option 82 at the service port level.

    2. On the OLT, run the **dhcp-option82 permit-forwarding service-port** command with the **enable** parameter selected, to allow ONU DHCP packets to carry Option 82 information.

  - Enable Policy Information Transfer Protocol (PITP) on both the OLT and ONUs. This configuration is recommended for the PPPoE-based Internet access service.

    1. Enable PITP on both the OLT and ONUs.

       PITP can be enabled or disabled at four levels: global, port, VLAN, and service port levels. This function takes effect only after it is enabled at the four levels. Among the four levels, PITP is disabled only at the global level by default.

Copyright © Huawei Technologies Co., Ltd.

- The global level: In global config mode, run the **pitp enable pmode**, **pitp forward pmode**, or **pitp rebuild pmode** command to enable PITP at the global level.

  In the preceding commands, the **enable**, **forward**, and **rebuild** parameters can all enable PITP but provide different packet processing policies on the OLT. Select one of them based on site requirements. For details, see the **pitp** command.
- The port level: In global config mode, run the **pitp port** or **pitp board** command to enable PITP at the port level.
- The VLAN level:
  a. In global config mode, run the **vlan service-profile** command to create a VLAN service profile.
  b. Run the **pitp enable** command to enable PITP at the VLAN level.
  c. Run the **commit** command to make the profile configuration take effect.
  d. Run the **quit** command to quit the VLAN service profile mode.
  e. Run the **vlan bind service-profile** command to bind the created VLAN service profile to a VLAN.
- The service port level: In global config mode, run the **pitp service-port** command to enable PITP at the service port level.

2. On the OLT, run the **pitp permit-forwarding service-port** command with the **enable** parameter selected, to allow ONU PPPoE packets to carry a vendor tag.

----End

11.3.4.13 Configuring the Internet Access Service (on the HGW)

This topic describes how to configure the Internet access service for residential users on a home gateway (HGW) when the HGW is connected to an ONU upstream through a local area network (LAN) or in xDSL mode.

Context

Residential users generally access the Internet in Point-to-Point Protocol over Ethernet (PPPoE) dial-up mode. PPPoE dial-up can be performed on personal computers (PCs) or HGWs.

The configuration processes on HGWs of different models or in different appearances are similar. This topic describes how to configure the Internet access service on an HG239 that is connected to an ONU upstream through a LAN and on an HG527 that is connected to an ONU upstream in ADSL2+ mode.

Procedure

- Configure the Internet access service (on an HG239).
  1. Log in to the Web configuration window.
     a. Enter http://192.168.1.1/cu.html (default IP address) to the address bar of the Internet Explorer (IE) and press Enter.

Copyright © Huawei Technologies Co., Ltd.

b. In the login dialog box, enter the user name and password of the administrator (the Internet service provider (ISP) provides the default user name and default password). Then, click **OK**.

2. Set parameters for the Internet access service.

   Assume that ports LAN1 and LAN2 are Internet access ports for PCs.

   a. Choose **Network** > **Bandwidth Configuration** from the navigation tree.

   b. Create WAN connection 1 and set parameters based on the following table.

Parameter	Value
Bearing service	INTERNET
VLAN enabling	Enabled: Upstream packets contain VLAN tags. Disabled: Upstream packets do not contain VLAN tags. **NOTE** If **uservlan** is set to **untagged** when you configure a service flow for the Internet access service on the ONU, set this parameter to **Disabled**; otherwise, set it to **Enabled**.
VLANID [1-4094]	If **VLAN enabling** is set to **Enabled**, this parameter takes the value of **uservlan** that is specified when you configure a service flow for the Internet access service on the ONU.
Binding item	LAN1 and LAN2: PCs connected to ports LAN1 and LAN2 can simultaneously access the Internet.
Mode	Bridge: PCs access the Internet in PPPoE dial-up mode.

   c. Click **OK**.

3. Restart the HGW.

   Choose **Management** > **Device Management** and click **Restarting the Device**.

- Configure the Internet access service (on an HG527).

  1. Log in to the Web configuration window.

     a. Enter http://192.168.1.1/cnc.html (default IP address) to the address bar of the IE and press Enter.

     b. In the login dialog box, enter the user name (default: admin) and password (default: admin) of the administrator. Then, click **OK**.

  2. Set parameters for the Internet access service.

     Assume that ports LAN1 and LAN2 are Internet access ports for PCs.

     a. Choose **Network** > **Bandwidth Configuration** from the navigation tree.

     b. Create WAN connection 1 and set parameters based on the following table.

Parameter	Value
Bearing service	INTERNET

Copyright © Huawei Technologies Co., Ltd.

Parameter	Value
Enabling	If this parameter is selected, WAN connection 1 is used.
VPI/VCI	Contact your carrier for the value ranges of VPIs and VCIs. Ensure that the VPI/VCI setting (for example, 0/35) on an HGW is consistent with that on the office to which the HGW is connected.
Binding item	LAN1 and LAN2: PCs connected to ports LAN1 and LAN2 can simultaneously access the Internet.
Mode	Bridge: PCs access the Internet in PPPoE dialup mode.
Encapsulation mode	LLC

c. Click **OK**.

3. Restart the HGW.

   Choose **Management** > **Device Management** and click **Restarting the Device**.

----End

11.3.4.14 Configuring the IPTV Service (on the HGW)

This topic describes how to configure the IPTV service on the HGW that uses LAN or xDSL for upstream transmission. This configuration enables home subscribers to watch IPTV programs using STBs and TVs.

Context

HGWs have different models and appearances but their configuration procedures are similar. This topic uses the HG239 that uses LAN for upstream transmission and the HG527 that uses ADSL2+ for upstream transmission as examples.

Procedure

- Configure the IPTV service on the HG239.
  1. Log in to the Web configuration window.
     a. Enter http://192.168.1.1/cu.html (default IP address) to the address bar of the Internet Explorer (IE) and press Enter.
     b. In the login dialog box, enter the user name and password of the administrator (the Internet service provider (ISP) provides the default user name and default password). Then, click **OK**.
  2. Configure multicast parameters.

     This example assumes LAN 4 as an IPTV port.

     a. Choose **Network** > **Bandwidth Configuration** from the navigation tree.
     b. In the right pane, create LAN connection 2 for the IPTV service. Set the parameters as follows:

Copyright © Huawei Technologies Co., Ltd.

Parameter	Value
Bearing service	**OTHER**: The connection is used for the IPTV service.
VLAN enabling	**Enable** VLAN tags are added to upstream packets. **NOTE** When multicast service flows are created on the ONU, the value is **Disable** if **uservlan** is untagged and the value is **Enable** if **uservlan** is tagged.
VLANID [1-4094]	Multicast VLAN ID corresponding to the user VLAN value for multicast service flows created on the ONU. In this example, set this parameter to 43.
Binding item	LAN4
Mode	Bridge
DHCP transparent transmission	Enable

c. Click **OK** to save the settings.

3. Restart the HGW.

   Choose **Management** > **Device Management** and click **Restarting the Device**.

- Configure the IPTV service on the HG527.

1. Log in to the Web configuration window.

   a. Enter http://192.168.1.1/cnc.html (default IP address) to the address bar of the IE and press Enter.

   b. In the login dialog box, enter the user name (default: admin) and password (default: admin) of the administrator. Then, click **OK**.

2. Configure multicast parameters.

   This example assumes LAN 4 as an IPTV port.

   a. Choose **Network** > **Bandwidth Configuration** from the navigation tree.

   b. In the right pane, create LAN connection 1 for dialup Internet access services. Set the parameters as follows:

Parameter	Value
Bearing service	**OTHER**: The connection is used for the IPTV service.
Enabling	The LAN connection is enabled when this check box is selected.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Value
VLAN enabling	**Enable**: VLAN tags are added to upstream packets. **NOTE** When multicast service flows are created on the ONU, the value is **Disable** if **uservlan** is untagged and the value is **Enable** if **uservlan** is tagged.
VLANID [1-4094]	Multicast VLAN ID on the HGW when multicast service flows are created on the ONU. In this example, set this parameter to **43**.
VPI/VCI	Set the VPI/VCI to the same as that configured on the devices at the central office. In this example, set this parameter to **0/35**.
Binding item	LAN4
Mode	Bridge
Encapsulation mode	LLC

c. Click **OK** to save the settings.

3. Restart the HGW.

   Choose **Management** > **Device Management** and click **Restarting the Device**.

----End

11.3.4.15 Configuring the VoIP Service (on the HGW)

This topic describes how to configure the voice service on HGWs that use LAN or xDSL for upstream transmission. This configuration enables home subscribers to enjoy the POTS service by using an analog telephone.

Context

HGWs have different models and appearances but their configuration procedures are similar. This topic uses the HG255 that uses LAN for upstream transmission and the HG555 that usesADSL2+ for upstream transmission as examples.

The IADs use SIP as the voice protocol.

Procedure

- Configure the VoIP service on the HG255.
  1. Log in to the Web configuration interface.
     a. Enter **http://192.168.1.1** (default IP address) in the address bar of the browser and press Enter.
     b. In the login window, enter the user name and password (the default value is provided by ISP) of the administrator and click **OK**.

Copyright © Huawei Technologies Co., Ltd.

2. Configure parameters of the voice service.

   The configuration procedure is as follows:

   a. In the Web page, choose **Network** > **Bandwidth Configuration** from the navigation tree.

   b. Create WAN Connection 3 for the VoIP service and set the parameters as follows:

Parameter	Value
Bearing service	VoIP
Enabling status	Enable
VLAN mode	VLAN Transparent Transmission
VLAN ID	VLAN ID corresponding to the user VLAN value for voice service flows created on the ONU. In this example, set this parameter to 200.
802.1p	Enabled
Mode	Route: route mode
DHCP	Enabled
NAT	Enabled

   c. Click **OK** to save the settings.

   d. Choose **Appliciation** > **Broadband Phone Configuration** from the navigation tree. Configure the parameters as follows:

Parameter	Value
Address	Preferred IP address of the proxy server: 200.200.200.200
Port ID	Preferred signaling port ID of the proxy server: 5060
Enabling	Enabled
User number	When logging in to a VoIP account, you can set the user account to the user telephone number. In this example, set the user telephone number to 83110001.
User password	-

3. Restart the HGW.

   Choose **Management** > **Device Management** and click **Restarting the Device**.

- Configure the VoIP service (HG555)

  1. Log in to the Web configuration interface.

Copyright © Huawei Technologies Co., Ltd.

a. Enter **http://192.168.1.1** (default IP address) in the address bar of the browser and press Enter.

b. In the login window, enter the user name and password (the default value is provided by ISP) of the administrator and click **OK**.

2. Configure parameters of the voice service.

   The configuration procedure is as follows:

   a. Click **Appliciation** > **Broadband Phone Configuration** from the navigation tree.

   b. Create WAN Connection 3 for the VoIP service and set the parameters as follows:

Parameter	Value
Bearing service	VoIP
Enabling status	Implement
VPI/VCI	Set the VPI/VCI to the same as that configured on the devices at the central office. In this example, set this parameter to 0/35.
VLAN mode	VLAN Transparent Transmission
VLAN ID	VLAN ID corresponding to the user VLAN value for voice service flows created on the ONU. In this example, set this parameter to 200.
802.1p	Enabled
Mode	Route mode
DHCP	Enabled
NAT	Enabled

   c. Click OK.

   d. Choose **Appliciation** > **Broadband Phone Configuration** from the navigation tree. Configure the parameters as follows:

Parameter	Value
Address	Preferred IP address of the proxy server: 200.200.200.200
Port ID	Preferred signaling port ID of the proxy server: 5060
Enabling	Enabled
User number	When logging in to a VoIP account, you can set the user account to the user telephone number. In this example, set the user telephone number to 83110001.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Value
User password	-

3. Restart the HGW.
   Choose **Management** > **Device Management** and click **Restarting the Device**.

----End

11.3.4.16 Verifying Services

This topic describes the remote verification methods in the FTTB+HGW scenario (HGW providing the VoIP service). ONUs provide remote service verification methods including PPPoE dialup emulation and multicast emulation for configuration and commissioning engineers to verify services remotely after service configuration, avoiding a second on-site operation.

Prerequisites

ONUs and upper-layer devices are connected properly. The BRAS and MGC/IMS have been configured.

Context

This topic describes the remote verification method for different service.

NOTE

The VoD service and HGW VoIP service currently do not support remote verification.

Remote Service Verification Method	Function	Remarks
PPPoE dialup emulation	An ONU emulates a PPPoE user terminal software to perform dialup and interact with the BRAS to verify the connectivity between the ONT and BRAS.	● PPPoE dialup emulation requires a service flow which does not belong to a QinQ VLAN. ● A user name, password, and authentication mode must be configured on the BRAS for the PPPoE dialup emulation. ● An ONU supports a maximum of one PPPoE dialup emulation.

Copyright © Huawei Technologies Co., Ltd.

Remote Service Verification Method	Function	Remarks
Multicast emulation	This function enables you to emulate a multicast user goes online and lead the program stream to an ONU. By querying the real-time traffic of the multicast program, you can check whether the multicast function is performing well.	The multicast service configured in dynamic controllable multicast mode does not support the remote acceptance function.

Data plan

Item	Data	Remarks
PPPoE dialup emulation parameter	Referenced service flow ID: 101 Emulation timeout time: 10s	The entered user name, password, and authentication mode must be consistent with those configured on the BRAS.
Multicast emulation parameter	Multicast service flow ID: 401 Multicast VLAN: 1000 IP address of the multicast program: 224.1.1.10	-

Procedure

- Verify the Internet access service using PPPoE dialup emulation.
  1. Start an emulation test by running the **simulate dhcp start** command.

```
huawei(config)#pppoe simulate start
  Command:
          pppoe simulate start
 Service-port(index<0-999>):101
 User Name(length<1,65>):user0
 User Password(length<0,16>):*******
 Authentication Mode:
 1. Chap  2. Pap [default 1]:1
 Overtime Time(5-60s)[default 5]:10
```

  2. Query the emulation test information by running the **display pppoe simulate info** command.

```
huawei(config)#display pppoe simulate info
  PPPoE simulate information is:
  ------------------------------------------------------------------
  Service-port:  101
  User name:     user0
  Current phase: -                     //*Emulation phase
  Result:        Success               //*Emulation result
  Start time:    2011-11-16 15:41:29+08:00
```


Copyright © Huawei Technologies Co., Ltd.

```
  End time:      2011-11-16 15:41:34+08:00
  Session ID:    591
  User IP:       192.168.50.2
  Gateway IP:    192.168.50.254
  ------------------------------------------------------------------
```

3. Terminate the emulation test by running the **simulate dhcp start** command.

```
huawei(config)#pppoe simulate stop
```

- Verify the multicast service using multicast emulation.

1. Run the **igmp static-join** command to order a multicast program by emulating a multicast user.

```
huawei(config)#btv
huawei(config-btv)#igmp static-join service-port 401 ip 224.1.1.10 vlan
1000
```

2. Run the **display igmp use** command to query the status of the multicast user.

```
huawei(config-btv)#display igmp user service-port 401
  User                       : 0/3/1 //*Use an ETH port as an example.
  State                      : online
  Authentication             : no-auth
  Quick leave                : MAC-based
  IGMP flow ID               : 0
  Video flow ID              : 0
  Log switch                 : enable
  Bind profiles              : -
  IGMP version               : IGMP v3
  Available programs         : 91
  Global Leave               : disable
  User MaxBandWidth          : no-limit
  Used bandwidth(kbps)       : 5000
  The percentage of used
  bandwidth to port rate(%)  : -
  Total video bandwidth      : -
  Mcast video bandwidth      : -
  Active program list

------------------------------------------------------------------------
--
  Program name     VLAN  IP/MAC           State           Start-time

------------------------------------------------------------------------
--
  program1         1000  224.1.1.10       watching        2011-07-13
                                                         14:41:18

------------------------------------------------------------------------
--
  Total: 1
```

3. Run the **display multicast flow-statistic** command to query the real-time traffic of the multicast program.

```
huawei(config-btv)#display multicast flow-statistic ip 224.1.1.10 vlan
1000
  Command is being executed, please wait...
  Multicast flow statistic result: 360(kbps)
```

- Verify the VoD service.

1. Run the **display mac-address service-port** command on the ONU to query learned MAC addresses of VoD users. The learned MAC addresses of VoD users indicate that services are functioning properly between the ONU and VoD users.

   If the VPI/VCI is 0/35 and the ADSL2+ port is 0/2/0, run the following command to query the learned MAC addresses of VoD users:

Copyright © Huawei Technologies Co., Ltd.

```
huawei(config)#display mac-address service-port 301

  Command:
          display mac-address service-port 301

------------------------------------------------------------------------
-
  SRV-P BUNDLE TYPE MAC            MAC TYPE F /S /P  VPI  VCI
VLANID
  INDEX INDEX

------------------------------------------------------------------------
-
    301    -   adl 1010-1010-1000  dynamic  0 /2 /0  0    35          300

------------------------------------------------------------------------
-
  Total: 1
  Note: F--Frame, S--Slot, P--Port,
        VPI indicates ONT ID for PON, VCI indicates GEM index for GPON,
        v/e--vlan/encap, pri-tag--priority-tagged,
        ppp--pppoe, ip--ipoe, ip6--ipv6oe
```

2. On the OLT, run the **display mac-address vlan** command to query the learned ONU MAC addresses. The learned ONU MAC addresses indicate that services are functioning properly between the OLT and ONUs.

- Verify the VoIP service.
  1. Log in to the HGW management web page.

     For details, see the **11.3.4.15 Configuring the VoIP Service (on the HGW)**.
  2. Choose **Status** > **Broadband VoIP Information** to query the service registration status and telephone number.

     Expected service registration status: Register successfully.

----End

11.4 Configuring Services in Various FTTB and FTTC Scenarios (Ethernet Cascading)

This section describes how to configure services when a multi-dwelling unit (MDU) serving as an independent node or GE remote extended subrack cascades with an optical line terminal (OLT)through Ethernet port.

11.4.1 FTTB and FTTC Ethernet Cascade Networking (ONU Works as an Independent NE)

Cascade a multi-dwelling unit (MDU) to an optical line terminal (OLT) using an Ethernet access board, the MDU works as an independent NE. The following topics describe the configuration method of this scenario.

11.4.1.1 Service Requirements and Usage Scenario

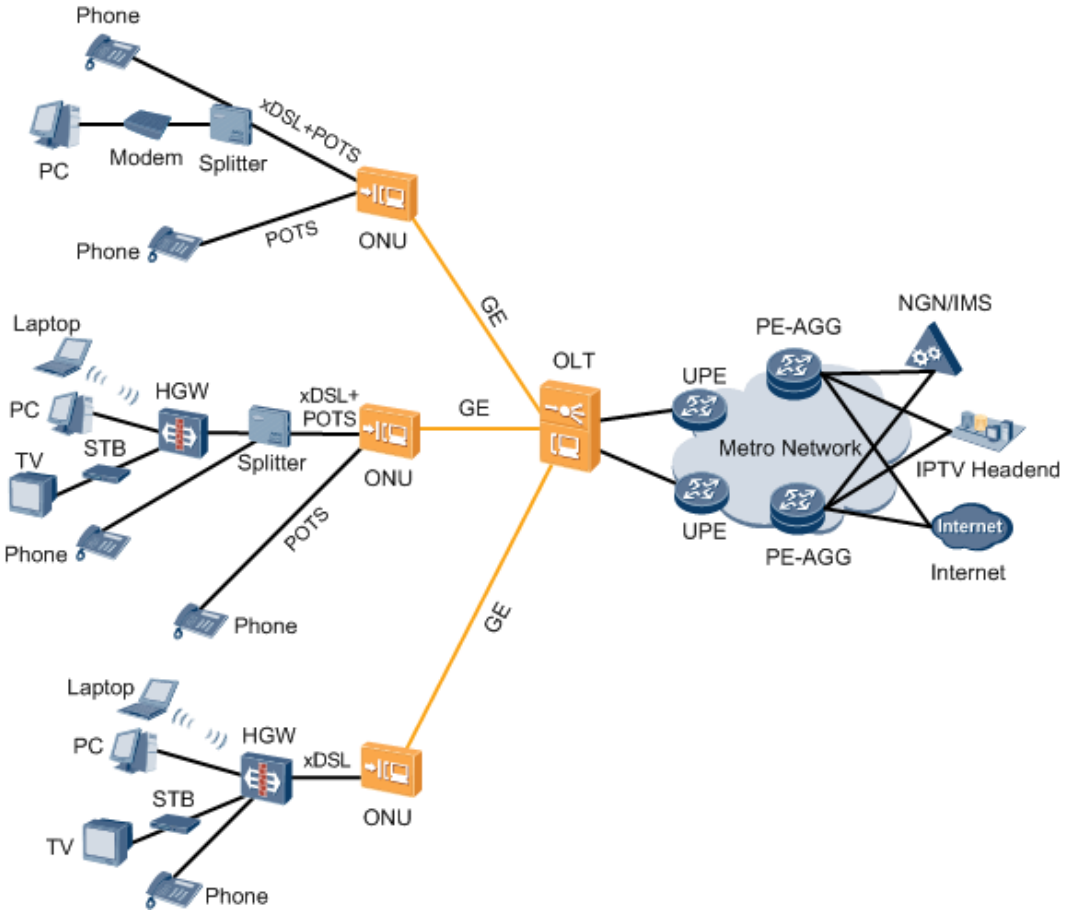
If an optical network unit (ONU) works as an independent NE on a fiber to the building (FTTB) or fiber to the curb (FTTC) Ethernet cascading network, the service requirements and usage

Copyright © Huawei Technologies Co., Ltd.

scenario of this network are the same as those of a PON network. The differences lie in the ONU upstream transmission mode and the user access mode. Specifically, on an FTTB or FTTC Ethernet cascading network, an ONU connects to the optical line terminal (OLT) through an Ethernet port and users connect to the ONU through xDSL lines; on a PON network, an ONU connects to the OLT through a PON port and users connect to the ONU through optical lines.

Networking Scenario	Service Requirements and Usage Scenario
FTTB/FTTC Networking (xDSL Access Without HGW)	See **11.3.2.1 Service Requirements and Application Scenario**. For the networking diagram, the Ethernet cascading network does not need the optical splitter.
FTTB/FTTC+HGW Networking (ONU Providing the VoIP Service)	See **11.3.3.1 Service Requirements and Application Scenario**. Focus only on the xDSL access. For the networking diagram, the Ethernet cascading network does not need the optical splitter.
FTTB/FTTC+HGW Networking (HGW Providing the VoIP Service)	See **11.3.4.1 Service Requirements and Application Scenario**. Focus only on the xDSL access. For the networking diagram, the Ethernet cascading network does not need the optical splitter.

The following figure shows the networking in the preceding scenarios.

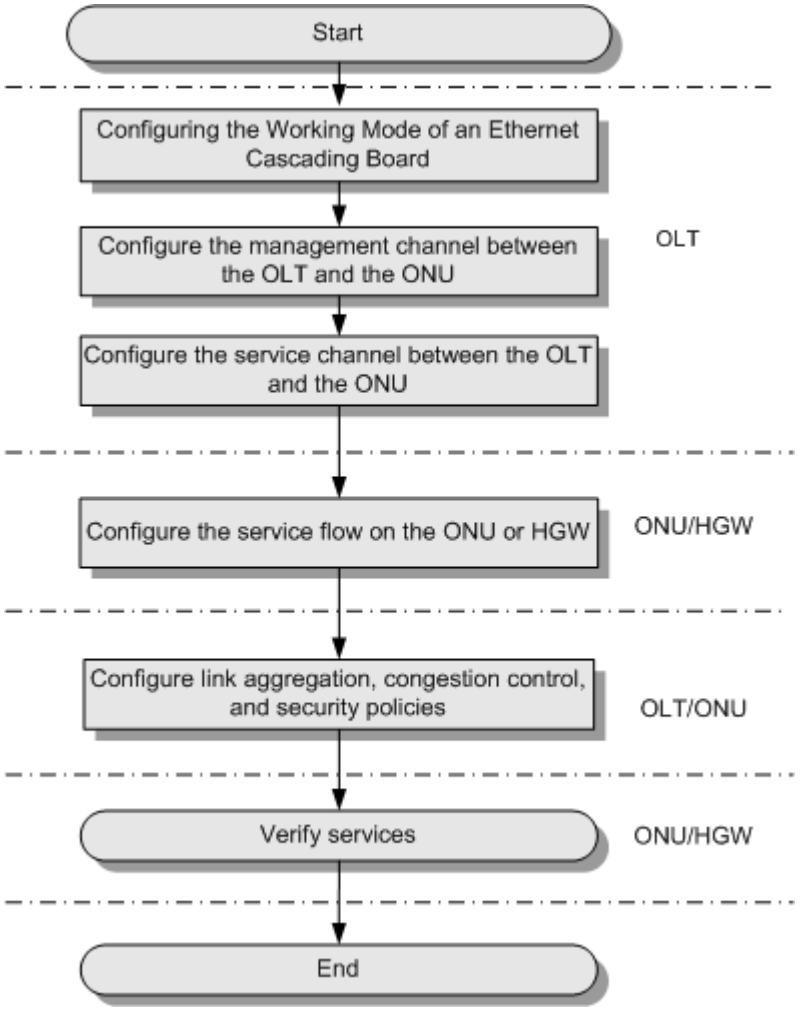


Copyright © Huawei Technologies Co., Ltd.

11.4.1.2 Configuration Procedure

Figure 11-11 shows the configuration procedure for a fiber to the building (FTTB) or fiber to the curb (FTTC) Ethernet cascading network where an optical network unit (ONU) works as an independent NE.

Figure 11-11 Configuration process for an FTTB or FTTC Ethernet cascading network where an ONU works as an independent NE



The following table describes the configuration steps.

Configuration Object	Step	Description
Optical line terminal (OLT)	**Configure the working mode of an Ethernet cascading board.**	An Ethernet cascading board supports various working modes. Configure the working mode to **cascade** in this scenario.

Copyright © Huawei Technologies Co., Ltd.

Configuration Object	Step	Description
	Configure the management channel between the OLT and the ONU.	After the inband management channel between the OLT and the ONU is configured and available, you can log in to the ONU from the OLT to configure the ONU. If the remote software commissioning using GE upstream transmission is required, configure the management channel on the OLT. If the remote software commissioning using GE upstream transmission is not required, configure the management channel on both the OLT and the ONU. The configuration object listed in this table is only the main object.
	Configure the service channel between the OLT and the ONU.	Configure a channel on the OLT for the Internet access service, voice service, or IPTV service.
ONU Home gateway (HGW)	**Configure the service flow on the ONU or HGW.**	Configure the service flow based on site requirements.
OLT ONU	**Configure link aggregation, congestion control, and security policies.**	The global configuration of upstream link aggregation and queue scheduling based on priorities ensures service reliability. The global configuration of security policies ensures service security.
ONU HGW	**Verify services.**	ONUs support remote service verification methods, such as PPPoE dialup, call, and multicast service emulation tests. This allows commissioning and configuration engineers to remotely verify services. The voice service on the HGW does not support remote verification.

11.4.1.3 Configuring the Working Mode of an Ethernet Cascading Board

This section describes how to configure the working mode of an Ethernet cascading board to **cascade**. After the configuration, an optical network unit (ONU) can cascade with an optical line terminal (OLT) equipped with the Ethernet cascading board.

Data Plan

Item	Data
ETHB cascading board	Cascading port: 0/3/0

Copyright © Huawei Technologies Co., Ltd.

Item	Data
OPGD cascading board	Cascading port: 0/2/0

Procedure

- Configure the working mode of an ETHB cascading board to **cascade**.

```
huawei(config)#interface eth 0/3
huawei(config-if-eth-0/3)#network-role cascade
huawei(config-if-eth-0/3)#quit
```

NOTICE

If the working mode of the ETHB cascading board was originally **extend**, the board restarts after this operation is performed.

- Configure the working mode of an OPGD cascading board to **cascade**.

```
huawei(config)#interface opg 0/2
huawei(config-if-opg-0/2)#network-role cascade
huawei(config-if-opg-0/2)#quit
```

----End

11.4.1.4 Configuring the Management Channel Between an OLT and an ONU

This section describes how to configure a management channel between an optical line terminal (OLT) and an optical network unit (ONU). After the configuration, you can log in to the ONU from the OLT and configure the ONU.

Context

FTTx V100R012 or later supports remote software commissioning using GE upstream transmission. Similar to the remote software commissioning function supported by a PON network, the remote software commissioning using GE upstream transmission implements one site visit for newly deployed GE-upstream devices. Before using remote software commissioning using GE upstream transmission, learn the following prerequisites and notes.

Prerequisite

Version requirements:

- The OLT version is V800R012 or later.
- The ONU version is V800R312/V800R012 (for MA5603Ts and MA5608Ts) or later.
- On a cascading network consisting of multiple cascaded devices, all devices on the network meet the preceding version requirements. For example, the networking of a cascading network is as follows: OLT -> ONU -> ONU. If an ONU version is earlier than V800R312, the remote software commissioning using GE upstream transmission cannot be used on the network.

Networking requirements:

Copyright © Huawei Technologies Co., Ltd.

- If the ONU connects to the OLT not through a physical-layer transmission device, such as a switch, they are connected through a GE or 10GE port. If the ONU connects to the OLT through a physical-layer transmission device, such as a switch, the physical-layer transmission device supports untagged Ethernet packets (including IEEE 802.3ah OAM and LACP packets) and transparently transmits the optical port status parameter.
- Only IPv4 management channel parameters can be configured.

Precautions

- Do not enable the remote software commissioning using PON upstream transmission.
- Ensure that the database of a newly deployed device is empty. Otherwise, the remote software commissioning using GE upstream transmission cannot be used.
- On a network consisting of multiple cascaded devices, ensure that the upper-layer device of a newly deployed device has been commissioned and can be logged in.
- Only the network management parameters defined in SNMPv1 and SNMPv2 are supported.
- When the ONU automatically obtains management parameters, it automatically generates a default route that can be restored. However, the default route may not be proper in service configuration. Therefore, you are advised to add a new route and delete the default one after the ONU management channel is available.
- After the ONU automatically obtains management parameters, the remote software commissioning function is automatically disabled if configurations are issued to the ONU through the U2000. To modify the ONU management parameters, remotely log in to the ONU through the command line interface (CLI).

Configuration requirements for the networking of OLT -> MA5603T:

- Do not remotely configure active/standby load-sharing on the MA5603T. Otherwise, the management IP address of the MA5603T is deleted and you cannot remotely log in to the MA5603T any more.
- If the MA5603T uses an SPUA board for upstream transmission, manual aggregation for Ethernet ports cannot be configured on the OLT.

Configuration requirements for an OLT or ONU (an OLT is used as an example in the following description) connected to an ONU through a link aggregation group (LAG):

- Neighbor automatic communication (NAC) can be configured only on the master port in a LAG. When deploying a new device, ensure that the master port is correctly connected.
- The Link Aggregation Control Protocol (LACP) is recommended for an OLT LAG. For a manual static LAG, during remote commissioning, run the **shutdown** command to disable sub-ports in the LAG on the master node, manually configure a static LAG on the slave node, and then run the **undo shutdown** command to enable the sub-ports in the LAG on the master node.
- After the ONU goes online, remotely log in to the ONU and manually add a VLAN for the master port and sub-ports in the LAG.

Copyright © Huawei Technologies Co., Ltd.

Data Plan When Remote Software Commissioning Using GE Upstream Transmission Is Enabled

Configuration Item	Data	Remarks
Ethernet cascading port on the OLT	ETHB cascading board: 0/3/0 OPGD cascading board: 0/2/0	None
Management VLAN and IP address of the OLT	ID of the management VLAN: 8 Type of the management VLAN: smart Management IP address: 192.168.50.1/24	Here we take the scenario of "to remotely log in to the ONU from the OLT for configuration" for example, so we need to ensure that the management VLAN of the OLT is the same as that of the ONU and that the management IP address of the OLT is in the same network segment as that of the ONU.
Management VLAN and IP address of the ONU	ID of the management VLAN: 8 Type of the management VLAN: smart Management IP address: 192.168.50.2/24	
Management profile of the ONU	ID: 64 Name: snmp-profile_64 SNMP version: SNMPv2c	None

Data Plan When Remote Software Commissioning Using GE Upstream Transmission Is Disabled

Configuration Item	Data	Remarks
Ethernet cascading port on the OLT	ETHB cascading board: 0/3/0 OPGD cascading board: 0/2/0	None
Management VLAN and IP address of the OLT	ID of the management VLAN: 8 Type of the management VLAN: smart Management IP address: 192.168.50.1/24	Here we take the scenario of "to remotely log in to the ONU from the OLT for configuration" for example, so we need to ensure that the management VLAN of the OLT is the same as that of the ONU and that the management IP address of the OLT is in the same network segment as that of the ONU.
Management VLAN and IP address of the ONU	ID of the management VLAN: 8 Type of the management VLAN: smart Management IP address: 192.168.50.2/24	

Copyright © Huawei Technologies Co., Ltd.

Procedure

- Configure a management channel if the remote software commissioning using GE upstream transmission is enabled and the cascading board is ETHB.
  1. Configure the inband management VLAN and IP address of the OLT.

     The ID of the inband management VLAN is 8, the VLAN priority is 6, and the management IP address is 192.168.50.1/24.

     ```
     huawei(config)#vlan 8 smart
     huawei(config)#port vlan 8 0/19 0
     huawei(config)#vlan priority 8 6
     huawei(config)#interface vlanif 8
     huawei(config-if-vlanif8)#ip address 192.168.50.1 24
     huawei(config-if-vlanif8)#quit
     ```

  2. Add the cascading port to the management VLAN.

     ```
     huawei(config)#port vlan 8 0/3 0
     ```

  3. Enable NAC on the OLT.

     ```
     huawei(config)#nac enable master 0/3 0
     ```

  4. (Optional) Create an SNMP management profile.

     Perform this operation if the ONU is managed through the U2000. Plan an SNMP management profile on the U2000 and ONU before creating the profile.

     ```
     huawei(config)#snmp-profile add profile-id 64 profile-name snmp-
     profile_64 v2c public
     private 192.168.50.55 30000 trapstatus
     ```

  5. Configure ONU management parameters on the OLT.

     ```
     huawei(config)#nac config master 0/3/0 slave vlan 8 priority 3 ip-
     address
     192.168.50.2 mask 255.255.255.0 gateway 192.168.50.254 snmp-profile-id 64
     ```

     Check whether the ONU management parameters have been configured on the OLT.

     ```
     huawei(config)#display nac configuration master
     ```

  6. Upon power-on, the ONU exchanges data with the OLT to obtain the management parameters. Two minutes later, run the **telnet** command to remotely log in to the ONU.
  7. Query the device connected to the cascading port on the OLT.

     ```
     huawei(config)#display nac slave info detail
     ```

  8. (Optional) Disable NAC on the OLT.

     Perform this operation after the ONU obtains the management parameters. This prevents the OLT from issuing the originally planned data to a substituted ONU.

     ```
     huawei(config)#nac disable master 0/3 0
     ```

- Configure a management channel if the remote software commissioning using GE upstream transmission is enabled and the cascading board is OPGD.
  1. Configure the inband management VLAN and IP address of the OLT.

     The ID of the inband management VLAN is 8, the VLAN priority is 6, and the management IP address is 192.168.50.1/24.

     ```
     huawei(config)#vlan 8 smart
     huawei(config)#port vlan 8 0/19 0
     huawei(config)#vlan priority 8 6
     huawei(config)#interface vlanif 8
     huawei(config-if-vlanif8)#ip address 192.168.50.1 24
     huawei(config-if-vlanif8)#quit
     ```


Copyright © Huawei Technologies Co., Ltd.

2. Configure the inband management service flow.

   The index of the service flow is 1. The ID of the management VLAN is 8. The Ethernet cascading port is 0/2/0. The ID of the user-side VLAN is 8. The OLT does not limit the rate of the inband management service flow. Therefore, use the default traffic profile with ID 6, which does not limit the rate of a service flow.

   ```
   huawei(config)#service-port 1 vlan 8 eth 0/2/0 multi-service user-vlan 8
   rx-cttr 6 tx-cttr 6
   ```

3. Enable NAC on the OLT.

   ```
   huawei(config)#nac enable master 0/2 0
   ```

4. (Optional) Create an SNMP management profile.

   Perform this operation if the ONU is managed through the U2000. Plan an SNMP management profile on the U2000 and ONU before creating the profile.

   ```
   huawei(config)#snmp-profile add profile-id 64 profile-name snmp-
   profile_64 v2c public
   private 192.168.50.55 30000 trapstatus
   ```

5. Configure ONU management parameters on the OLT.

   ```
   huawei(config)#nac config master 0/2/0 slave vlan 8 priority 3 ip-
   address
   192.168.50.2 mask 255.255.255.0 gateway 192.168.50.254 snmp-profile-id 64
   ```

   Check whether the ONU management parameters have been configured on the OLT.

   ```
   huawei(config)#display nac configuration master
   ```

6. Upon power-on, the ONU exchanges data with the OLT to obtain the management parameters. Two minutes later, run the **telnet** command to remotely log in to the ONU.

7. Query the device connected to the cascading port on the OLT.

   ```
   huawei(config)#display nac slave info detail
   ```

8. (Optional) Disable NAC on the OLT.

   Perform this operation after the ONU obtains the management parameters. This prevents the OLT from issuing the originally planned data to a substituted ONU.

   ```
   huawei(config)#nac disable master 0/2 0
   ```

- Configure a management channel if the remote software commissioning using GE upstream transmission is disabled and the cascading board is ETHB.

  1. Configure the inband management VLAN and IP address of the ONU.

     Log in to the ONU through a local serial port and configure the ONU as follows: The ID of the inband management VLAN is 8 and the management IP address is 192.168.50.2/24.

     ```
     huawei(config)#vlan 8 smart
     huawei(config)#port vlan 8 0/0 0
     huawei(config)#interface vlanif 8
     huawei(config-if-vlanif8)#ip address 192.168.50.2 24
     huawei(config-if-vlanif8)#quit
     ```

  2. Configure the inband management VLAN and IP address of the OLT.

     The ID of the inband management VLAN is 8, the VLAN priority is 6, and the management IP address is 192.168.50.1/24.

     ```
     huawei(config)#vlan 8 smart
     huawei(config)#port vlan 8 0/19 0
     huawei(config)#vlan priority 8 6
     huawei(config)#interface vlanif 8
     ```


Copyright © Huawei Technologies Co., Ltd.

```
huawei(config-if-vlanif8)#ip address 192.168.50.1 24
huawei(config-if-vlanif8)#quit
```

3. Add the cascading port to the management VLAN.

```
huawei(config)#port vlan 8 0/3 0
```

4. Check whether the management channel between the OLT and the ONU is available.
   - Run the **ping *192.168.50.2*** command on the OLT to check the connectivity between the OLT and the ONU. If the OLT can receive Internet Control Message Protocol (ICMP) ECHO-REPLY packets sent from the ONU, the ONU is connected to the OLT.
   - If you can remotely log in to the ONU from the OLT for configuration, the ONU is connected to the OLT.

- Configure a management channel if the remote software commissioning using GE upstream transmission is disabled and the cascading board is OPGD.

1. Configure the inband management VLAN and IP address of the ONU.

   Log in to the ONU through a local serial port and configure the ONU as follows: The ID of the inband management VLAN is 8 and the management IP address is 192.168.50.2/24.

```
huawei(config)#vlan 8 smart
huawei(config)#port vlan 8 0/0 0
huawei(config)#interface vlanif 8
huawei(config-if-vlanif8)#ip address 192.168.50.2 24
huawei(config-if-vlanif8)#quit
```

2. Configure the inband management VLAN and IP address of the OLT.

   The ID of the inband management VLAN is 8, the VLAN priority is 6, and the management IP address is 192.168.50.1/24.

```
huawei(config)#vlan 8 smart
huawei(config)#port vlan 8 0/19 0
huawei(config)#vlan priority 8 6
huawei(config)#interface vlanif 8
huawei(config-if-vlanif8)#ip address 192.168.50.1 24
huawei(config-if-vlanif8)#quit
```

3. Configure the inband management service flow.

   The index of the service flow is 1. The ID of the management VLAN is 8. The Ethernet cascading port is 0/2/0. The ID of the user-side VLAN is 8. The OLT does not limit the rate of the inband management service flow. Therefore, use the default traffic profile with ID 6, which does not limit the rate of a service flow.

```
huawei(config)#service-port 1 vlan 8 eth 0/2/0 multi-service user-vlan 8
rx-cttr 6 tx-cttr 6
```

4. Check whether the management channel between the OLT and the ONU is available.
   - Run the **ping *192.168.50.2*** command on the OLT to check the connectivity between the OLT and the ONU. If the OLT can receive ICMP ECHO-REPLY packets sent from the ONU, the ONU is connected to the OLT.
   - If you can remotely log in to the ONU from the OLT for configuration, the ONU is connected to the OLT.

----End

Copyright © Huawei Technologies Co., Ltd.

11.4.1.5 Configuring the Service Channel Between an OLT and an ONU

This section describes how to configure a service channel between an optical line terminal (OLT) and an optical network unit (ONU). After the configuration, the service channel forwards service packets on the ONU at Layer 2 based on the planned VLAN and forwarding policy.

Data Plan and Configuration Description

Planning the service channel between an OLT and an ONU is planning VLAN data. The following table lists the data plan in various Ethernet cascading scenarios.

Networking Scenario	Data Plan and Configuration Procedure
FTTB/FTTC Networking (xDSL Access Without HGW)	Internet access service channel (Create a common S-VLAN on the OLT to transparently transmit the Internet access service packets from a stacking VLAN on the ONU. For details about VLAN planning principles, see **11.2.3 Principle of Internet Access Service Data Plan**): ● S-VLAN: 1001 ● C-VLAN (Internet access service S-VLAN on the ONU): 1001 Voice service channel (The OLT transparently transmits VLAN tags carried in voice service packets. For details about VLAN planning principles, see **11.2.5 Principle of VoIP Service Data Plan**): ● S-VLAN: 200 ● C-VLAN (Voice service S-VLAN on the ONU): 200

Copyright © Huawei Technologies Co., Ltd.

Networking Scenario	Data Plan and Configuration Procedure
FTTB/FTTC+HGW Networking (ONU Providing the VoIP Service)	Internet access channel (Create a common S-VLAN on the OLT to transparently transmit the Internet access service packets from a stacking VLAN on the ONU. For details about VLAN planning principles, see **11.2.3 Principle of Internet Access Service Data Plan**): ● S-VLAN: 1001 ● C-VLAN (Internet access service S-VLAN on the ONU): 1001 Voice service channel (The OLT transparently transmits VLAN tags carried in voice service packets from the ONU. For details about VLAN planning principles, see **11.2.5 Principle of VoIP Service Data Plan**): ● S-VLAN: 200 ● C-VLAN (Voice service S-VLAN on the ONU): 200 VoD service channel (The OLT transparently transmits VLAN tags carried in VoD service packets from the ONU. For details about VLAN planning principles, see **11.2.6 Principle of IPTV Service Data Plan**): ● S-VLAN: 300 ● C-VLAN (VoD service S-VLAN on the ONU): 300 Multicast service channel (The OLT functions as an IGMP proxy. For details about VLAN planning principles, see **11.2.6 Principle of IPTV Service Data Plan**): ● Multicast VLAN: 1000 ● Multicast cascading port: 0/3/0 (ETHB) or 0/2/0 (OPGD) ● IGMP version: IGMPv3 ● IGMP mode: IGMP proxy ● Multicast program library: 224.1.1.10-224.1.1.100 ● IP address of the multicast server: 10.10.10.10/24
FTTB/FTTC+HGW Networking (HGW Providing the VoIP Service)	See the description for "FTTB/FTTC+HGW networking (ONU providing the VoIP service)".

Based on the preceding data plan, the service channel configuration in "FTTB/FTTC+HGW networking (ONU providing the VoIP service)" involves the other two sub-scenarios. The following section uses this networking as an example to describe how to configure the channels.

Procedure

- Configure a service channel if the Ethernet cascading board is ETHB.

  If the Ethernet cascading board is ETHB, no service flow needs to be configured on the OLT. You only need to add the Ethernet cascading port (for example, 0/3/0) to each S-VLAN.

Copyright © Huawei Technologies Co., Ltd.

1. Configure a channel for the Internet access service.

   Create S-VLAN 1001 for the Internet access service and add uplink port 0/19/0 and Ethernet cascading port to the VLAN.

   ```
   huawei(config)#vlan 1001 smart
   huawei(config)#port vlan 1001 0/19 0
   huawei(config)#port vlan 1001 0/3 0
   ```

2. Configure a channel for the voice service.

   Create S-VLAN 200 for the voice service and add uplink port 0/19/0 and Ethernet cascading port to the VLAN.

   ```
   huawei(config)#vlan 200 smart
   huawei(config)#port vlan 200 0/19 0
   huawei(config)#port vlan 200 0/3 0
   ```

3. Configure a channel for the VoD service.

   Create S-VLAN 300 for the VoD service and add uplink port 0/19/0 and Ethernet cascading port to the VLAN.

   ```
   huawei(config)#vlan 300 smart
   huawei(config)#port vlan 300 0/19 0
   huawei(config)#port vlan 300 0/3 0
   ```

4. Configure a channel for the multicast service.

   Create S-VLAN 1000 for the multicast service and add uplink port 0/19/0 and Ethernet cascading port to the VLAN.

   ```
   huawei(config)#vlan 1000 smart
   huawei(config)#port vlan 1000 0/19 0
   huawei(config)#port vlan 1000 0/3 0
   ```

   Configure a multicast cascading port.

   ```
   huawei(config)#btv
   huawei(config-btv)#igmp cascade-port 0/3/0
   ```

   Configure the IGMP version.

   ```
   huawei(config)#multicast-vlan 1000
   huawei(config-mvlan1000)#igmp version v3
   ```

   Configure the IGMP mode.

   ```
   huawei(config-mvlan1000)#igmp mode proxy
     Are you sure to change IGMP mode?(y/n)[n]:y
   ```

   Configure a multicast uplink port.

   ```
   huawei(config-mvlan1000)#igmp uplink-port 0/19/0
   ```

   Configure multicast programs.

   ```
   huawei(config-mvlan1000)#igmp program add batch ip 224.1.1.10 to-ip
   224.1.1.100
    sourceip 10.10.10.10
   ```

- Configure a service channel if the Ethernet cascading board is OPGD.

  If the Ethernet cascading board is OPGD, service flows must be configured on the OLT. The following configurations uses the Ethernet cascading port 0/2/0 on the OPGD board as an example.

  1. Configure a channel for the Internet access service.

     Create VLAN 1001 for the Internet access service and add uplink port 0/19/0 to the VLAN.

     ```
     huawei(config)#vlan 1001 smart
     huawei(config)#port vlan 1001 0/19 0
     ```

     Configure a traffic profile for the service flow. (The 802.1p priority of the Internet access service is 0 and the traffic profile does not limit rates. You can run the **display**

Copyright © Huawei Technologies Co., Ltd.

traffic table ip command to query the traffic profiles existing in the system. Traffic profile 6 meets the requirements and you do not need to configure it.)

```
huawei(config)#display traffic table ip from-index 0
```

Configure a service flow to receive and transparently transmit the Internet access service packets from the ONU.

```
huawei(config)#service-port vlan 1001 eth 0/2/0 multi-service user-vlan
1001
tag-transform transparent rx-cttr 6 tx-cttr 6
```

2. Configure a channel for the voice service.

   Create VLAN 200 for the voice service and add uplink port 0/19/0 to the VLAN.

   ```
   huawei(config)#vlan 200 smart
   huawei(config)#port vlan 200 0/19 0
   ```

   Configure a traffic profile for the service flow. (The 802.1p priority of the voice service is 5 and the traffic profile does not limit rates. You can run the **display traffic table ip** command to query the traffic profiles existing in the system. No traffic profile meets the requirements and create traffic profile 9, where *priority-policy* is set to **local-setting**, indicating that queues are scheduled based on the priority specified in the traffic profile.)

   ```
   huawei(config)#traffic table ip index 9 cir off priority 5 priority-policy
   local-setting
   ```

   Configure a service flow to receive and transparently transmit the voice service packets from the ONU.

   ```
   huawei(config)#service-port vlan 200 eth 0/2/0 multi-service user-vlan
   200
   tag-transform transparent rx-cttr 9 tx-cttr 9
   ```

3. Configure a channel for the VoD service.

   Create VLAN 300 for the VoD service and add uplink port 0/19/0 to the VLAN.

   ```
   huawei(config)#vlan 300 smart
   huawei(config)#port vlan 300 0/19 0
   ```

   Configure a traffic profile for the service flow. (The 802.1p priority of the VoD service is 4 and the traffic profile does not limit rates. You can run the **display traffic table ip** command to query the traffic profiles existing in the system. No traffic profile meets the requirements and create traffic profile 10, where *priority-policy* is set to **local-setting**, indicating that queues are scheduled based on the priority specified in the traffic profile.)

   ```
   huawei(config)#traffic table ip index 10 cir off priority 4 priority-
   policy local-Setting
   ```

   Configure a service flow.

   ```
   huawei(config)#service-port vlan 300 eth 0/2/0 multi-service user-vlan
   300
   tag-transform transparent rx-cttr 10 tx-cttr 10
   ```

4. Configure a channel for the multicast service.

   Create VLAN 1000 for the multicast service and add uplink port 0/19/0 to the VLAN.

   ```
   huawei(config)#vlan 1000 smart
   huawei(config)#port vlan 1000 0/19 0
   ```

   Create a multicast service flow.

   ```
   huawei(config)#service-port vlan 1000 eth 0/2/0 multi-service user-vlan
   1000
   tag-transform transparent rx-cttr 10 tx-cttr 10
   ```

   Configure a multicast cascading port.

Copyright © Huawei Technologies Co., Ltd.

```
huawei(config)#btv
huawei(config-btv)#igmp cascade-port 0/2/0
```

Configure the IGMP version.

```
huawei(config)#multicast-vlan 1000
huawei(config-mvlan1000)#igmp version v3
```

Configure the IGMP mode.

```
huawei(config-mvlan1000)#igmp mode proxy
  Are you sure to change IGMP mode?(y/n)[n]:y
```

Configure a multicast uplink port.

```
huawei(config-mvlan1000)#igmp uplink-port 0/19/0
```

Configure multicast programs.

```
huawei(config-mvlan1000)#igmp program add batch ip 224.1.1.10 to-ip
224.1.1.100
 sourceip 10.10.10.10
```

----End

11.4.1.6 Configuring the Service Flow on an ONU or HGW

This section describes how to configure the service flow on an optical network unit (ONU) or a home gateway (HGW) to provide a user service.

Data Plan and Configuration Description

The data plan and configuration method for the Internet access service on an ONU or HGW in Ethernet cascading scenarios are different from those in PON scenarios. The reason is as follows: In Ethernet cascading scenarios, data is encapsulated in S-VLAN+C-VLAN mode on the ONU and the OLT transparently transmits the S-VLAN tag (C-VLAN tag for the OLT) carried in ONU packets. Each ONU uses an S-VLAN and it differentiates users by C-VLAN. In addition, the user access modes are different. Specifically, in Ethernet cascading scenarios, users are connected to the ONU through xDSL lines; in PON scenarios, users are connected to the ONU through optical lines.

Copyright © Huawei Technologies Co., Ltd.

Networking Scenario	Data Plan and Configuration Procedure

FTTB/FTTC networking (xDSL access without an HGW)	For details, see:
	● **11.3.2.7 Configuring the Internet Access Service (VDSL2 Access, on the ONU)**
	The configurations in steps 3 and 4 are modified as follows (the configurations in other steps remain unchanged):
	– 3. Create an S-VLAN.
	Configure stacking S-VLAN 1001 for the ONU and add uplink port 0/0/1 to the VLAN.
	`huawei(config)#vlan 1001 smart`
	`huawei(config)#vlan attrib 1001 stacking`
	`huawei(config)#port vlan 1001 0/0 1`
	– 4. Add service ports.
	VDSL2 mode PTM and untagged user packets are used as an example. Add a service port for the users connected to ports 0/1/0 and 0/1/1, respectively.
	`huawei(config)#service-port 101 vlan 1001 vdsl mode ptm 0/1/0 multi-service user-vlan untagged`
	`tag-transform add-double inner-vlan 2 rx-cttr 8 tx-cttr 8 //Users are differentiated by C-VLAN (inner-vlan). Therefore, the C-VLAN (inner-vlan) of each user must be unique.`
	`huawei(config)#service-port 102 vlan 1001 vdsl mode ptm 0/1/1 multi-service user-vlan untagged`
	`tag-transform add-double inner-vlan 3 rx-cttr 8 tx-cttr 8`
	● **11.3.2.8 (Optional) Configuring Vectoring**
	● **11.3.2.9 Configuring H.248 Voice Service (on the ONU)**
	● **11.3.2.10 Configuring SIP Voice Service (on the ONU)**

Copyright © Huawei Technologies Co., Ltd.

Networking Scenario	Data Plan and Configuration Procedure

FTTB/FTTC+HGW networking (ONU providing the VoIP service)	For details, see:
	● **11.3.3.8 Configuring the Internet Access Service (VDSL2 Access, on the ONU)**
	The configurations in steps 3 and 4 are modified as follows (the configurations in other steps remain unchanged):
	– 3. Create an S-VLAN.
	Configure stacking S-VLAN 1001 for the ONU and add uplink port 0/0/1 to the VLAN.
	`huawei(config)#vlan 1001 smart`
	`huawei(config)#vlan attrib 1001 stacking`
	`huawei(config)#port vlan 1001 0/0 1`
	– 4. Add service ports.
	VDSL2 mode PTM and untagged user packets are used as an example. Add a service port for the users connected to ports 0/1/0 and 0/1/1, respectively.
	`huawei(config)#service-port 101 vlan 1001 vdsl mode ptm 0/1/0 multi-service user-vlan untagged tag-transform add-double inner-vlan 2 rx-cttr 8 tx-cttr 8 //Users are differentiated by C-VLAN (inner-vlan). Therefore, the C-VLAN (inner-vlan) of each user must be unique.`
	`huawei(config)#service-port 102 vlan 1001 vdsl mode ptm 0/1/1 multi-service user-vlan untagged tag-transform add-double inner-vlan 3 rx-cttr 8 tx-cttr 8`
	● **11.3.2.8 (Optional) Configuring Vectoring**
	● **11.3.2.9 Configuring H.248 Voice Service (on the ONU)**
	● **11.3.2.10 Configuring SIP Voice Service (on the ONU)**

Copyright © Huawei Technologies Co., Ltd.

Networking Scenario	Data Plan and Configuration Procedure

FTTB/FTTC+HGW networking (HGW providing the VoIP service)	For details, see:
	● **11.3.4.8 Configuring the Internet Access Service (VDSL2 Access, on the ONU)**
	The configurations in steps 3 and 4 are modified as follows (the configurations in other steps remain unchanged):
	– 3. Create an S-VLAN.
	Configure stacking S-VLAN 1001 for the ONU and add uplink port 0/0/1 to the VLAN.
	`huawei(config)#vlan 1001 smart`
	`huawei(config)#vlan attrib 1001 stacking`
	`huawei(config)#port vlan 1001 0/0 1`
	– 4. Add service ports.
	VDSL2 mode PTM and untagged user packets are used as an example. Add a service port for the users connected to ports 0/1/0 and 0/1/1, respectively.
	`huawei(config)#service-port 101 vlan 1001 vdsl mode ptm 0/1/0 multi-service user -vlan untagged tag-transform add-double inner-vlan 2 rx-cttr 8 tx-cttr 8 //Users are differentiated by C-VLAN (inner-vlan). Therefore, the C-VLAN (inner-vlan) of each user must be unique.`
	`huawei(config)#service-port 102 vlan 1001 vdsl mode ptm 0/1/1 multi-service user -vlan untagged tag-transform add-double inner-vlan 3 rx-cttr 8 tx-cttr 8`
	● **11.3.2.8 (Optional) Configuring Vectoring**
	● **11.3.2.9 Configuring H.248 Voice Service (on the ONU)**
	● **11.3.2.10 Configuring SIP Voice Service (on the ONU)**

11.4.1.7 Configuring Link Aggregation, Congestion Control, and Security Policy

The global configuration of upstream link aggregation and queue scheduling based on priorities ensures service reliability. The global configuration of security policies ensures service security.

Context

Link aggregation provides a higher bandwidth and uplink reliability for optical line terminals (OLTs) by aggregating multiple uplink Ethernet ports to one link aggregation group (LAG). Link aggregation is recommended.

Congestion control places the packets to be sent from a port into multiple queues that are marked with different priorities. Then, the packets are sent based on queue priorities. Congestion control is recommended.

Security policies ensure system, user, and service security.

Copyright © Huawei Technologies Co., Ltd.

NOTE

Enable a service security function based on the service type. For details, see **11.2.7 Principle of Security Data Plan**.

Procedure

- Configure link aggregation.

  The following configurations are used as an example to configure link aggregation:

  - Uplink ports 0/19/0 and 0/19/1 are added to a LAG.
  - The two ports send packets upstream based on the packets' source MAC addresses.
  - The LAG works in Link Aggregation Control Protocol (LACP) static aggregation mode.

  ```
  huawei(config)#link-aggregation 0/19 0-1 ingress workmode lacp-static
  ```

- Configure queue scheduling.

  According to quality of service (QoS) planning principles, all packets are scheduled in strict priority (SP) mode and mapped to queues according to the packets' priorities. For details about QoS planning principles, see **11.2.2 Principle of QoS Data Plan**.

  ```
  huawei(config)#queue-scheduler strict-priority
  huawei(config)#cos-queue-map cos0 0 cos4 4 cos5 5 cos6 6
  ```

- Configure system security.
  - Enable deny of service (DoS) anti-attack on both the OLT and optical network units (ONUs).
    1. Run the **security anti-dos enable** command to globally enable DoS anti-attack.
    2. Run the **security anti-dos control-packet policy** command to configure a protocol packet processing policy that will be used when a DoS attack occurs.
    3. Run the **security anti-dos control-packet rate** command to configure the threshold for the rate of sending protocol packets to the CPU.
  - Enable IP address anti-attack on both the OLT and ONUs.

    Run the **security anti-ipattack enable** command to enable IP address anti-attack.
- Configure user security.
  - Enable MAC address anti-flapping on both the OLT and ONUs.

    Run the **security anti-macduplicate enable** command to enable MAC address anti-flapping.
  - Enable MAC address anti-spoofing on both the OLT and ONUs.
    1. In global config mode, run the **security anti-macspoofing enable** command to globally enable MAC address anti-spoofing.
    2. Enable MAC address anti-spoofing at VLAN level in global config mode or service profile mode:
       a. In global config mode, run the **security anti-macspoofing vlan** command to enable MAC address anti-spoofing.
       b. Perform the following operations to enable MAC address anti-spoofing in service profile mode:
          a. In global config mode, run the **vlan service-profile** command to create a VLAN service profile.

Copyright © Huawei Technologies Co., Ltd.

b. Run the **security anti-macspoofing enable** command to enable MAC address anti-spoofing at VLAN level.

c. Run the **commit** command to make the profile configuration take effect.

d. Run the **quit** command to quit the VLAN service profile mode.

e. Run the **vlan bind service-profile** command to bind the created VLAN service profile to a VLAN.

3. (Optional) Run the **security anti-macspoofing max-mac-count** command to set the maximum number of MAC addresses that can be bound to a service flow.

4. (Optional) Run the **security anti-macspoofing exclude** command to configure the types of packets for which MAC address anti-spoofing does not take effect, such as Internet Group Management Protocol (IGMP) packets.

- Enable IP address anti-spoofing on ONUs.

  IP address anti-spoofing can be enabled or disabled at three levels: global, VLAN, and service port levels. This function takes effect only after it is enabled at the three levels. Among the three levels, IP address anti-spoofing is disabled only at the global level by default.

  1. In global config mode, run the **security anti-ipspoofing enable** command to enable IP address anti-spoofing at the global level.
  2. In VLAN service profile mode, run the **security anti-ipspoofing enable** command to enable IP address anti-spoofing at the VLAN level.
  3. Run the **security anti-ipspoofing service-port** *serviceport-id* **enable** command to enable IP address anti-spoofing at the service port level.

- Configure service security.
  - Enable Dynamic Host Configuration Protocol (DHCP) Option 82 on both the OLT and ONUs. This configuration is recommended for the DHCP-based Internet access service.

    1. Enable DHCP Option 82 on both the OLT and ONUs.

       DHCP Option 82 can be enabled or disabled at four levels: global, port, VLAN, and service port levels. This function takes effect only after it is enabled at the four levels. Among the four levels, DHCP Option 82 is disabled only at the global level by default.

       - The global level: In global config mode, run the **dhcp option82** command to enable DHCP Option 82 at the global level.

         When you run this command, select the **enable**, **forward**, or **rebuild** parameter based on site requirements. The three parameters can all enable DHCP Option 82 but provide different packet processing policies on the OLT. For details, see the **dhcp option82** command.

       - The port level: In global config mode, run the **dhcp option82 port** or **dhcp option82 board** command to enable DHCP Option 82 at the port level.

       - The VLAN level:

         a. In global config mode, run the **vlan service-profile** command to create a VLAN service profile.

Copyright © Huawei Technologies Co., Ltd.

b. Run the **dhcp option82 enable** command to enable DHCP Option 82 at the VLAN level.

c. Run the **commit** command to make the profile configuration take effect.

d. Run the **quit** command to quit the VLAN service profile mode.

e. Run the **vlan bind service-profile** command to bind the created VLAN service profile to a VLAN.

- The service port level: In global config mode, run the **dhcp option82 service-port** command to enable DHCP Option 82 at the service port level.

2. On the OLT, run the **dhcp-option82 permit-forwarding service-port** command with the **enable** parameter selected, to allow ONU DHCP packets to carry Option 82 information.

- Enable Policy Information Transfer Protocol (PITP) on both the OLT and ONUs. This configuration is recommended for the PPPoE-based Internet access service.

1. Enable PITP on both the OLT and ONUs.

   PITP can be enabled or disabled at four levels: global, port, VLAN, and service port levels. This function takes effect only after it is enabled at the four levels. Among the four levels, PITP is disabled only at the global level by default.

   - The global level: In global config mode, run the **pitp enable pmode**, **pitp forward pmode**, or **pitp rebuild pmode** command to enable PITP at the global level.

     In the preceding commands, the **enable**, **forward**, and **rebuild** parameters can all enable PITP but provide different packet processing policies on the OLT. Select one of them based on site requirements. For details, see the **pitp** command.

   - The port level: In global config mode, run the **pitp port** or **pitp board** command to enable PITP at the port level.

   - The VLAN level:

     a. In global config mode, run the **vlan service-profile** command to create a VLAN service profile.

     b. Run the **pitp enable** command to enable PITP at the VLAN level.

     c. Run the **commit** command to make the profile configuration take effect.

     d. Run the **quit** command to quit the VLAN service profile mode.

     e. Run the **vlan bind service-profile** command to bind the created VLAN service profile to a VLAN.

   - The service port level: In global config mode, run the **pitp service-port** command to enable PITP at the service port level.

2. On the OLT, run the **pitp permit-forwarding service-port** command with the **enable** parameter selected, to allow ONU PPPoE packets to carry a vendor tag.

----End

11.4.1.8 Verifying Services

In fiber to the building (FTTB) or fiber to the curb (FTTC) scenarios, optical network units (ONUs) are deployed far from the central office (CO). To facilitate service verification, ONUs support remote service verification methods, such as PPPoE dialup, call, and multicast service

Copyright © Huawei Technologies Co., Ltd.

emulation tests. This allows commissioning and configuration engineers to remotely verify services.

Verification Methods

The method of verifying a service on an Ethernet cascading network is the same as that of verifying a service on a PON network.

Networking Scenario	Data Plan and Configuration Procedure
FTTB/FTTC Networking (xDSL Access Without HGW)	For details, see **11.3.2.12 Verifying Services**.
FTTB/FTTC+HGW Networking (ONU Providing the VoIP Service)	For details, see **11.3.3.16 Verifying Services**.
FTTB/FTTC+HGW Networking (HGW Providing the VoIP Service)	For details, see **11.3.4.16 Verifying Services**.

11.4.2 FTTB and FTTC Ethernet Cascade Networking (ONU works as a GE remote extended subrack)

Working with high bandwidth technologies, such as VDSL2 and Vectoring, GE remote extended subracks provide high bandwidth access for users over existing copper line networks. GE remote extended subracks can be connected to traditional VDSL2 modems to provide Internet access and voice services for users; or be connected to home gateways (HGWs) to provide Internet, voice, and IPTV services for home users.

11.4.2.1 Service Requirements and Application Scenarios for GE Remote Extended Subrack

Centric management for GE remote extended subracks is used on networks that require high bandwidth access without adding more standalone NEs.

Service Requirements

- If only high speed Internet (HSI) and voice services are required, use traditional VDSL2 modems for user access.
- If HSI, voice, and IPTV services are required, use HGWs for user access.

Application Scenarios

As shown in **Figure 11-12**, a GE remote extended subrack is deployed in a corridor or roadside fiber distribution terminal, like a remotely deployed service board of a master subrack and is directly managed by the master subrack. In the upstream direction, it is connected to the master subrack through GE fibers; in the downstream direction, it is connected to user terminals through twisted pairs.

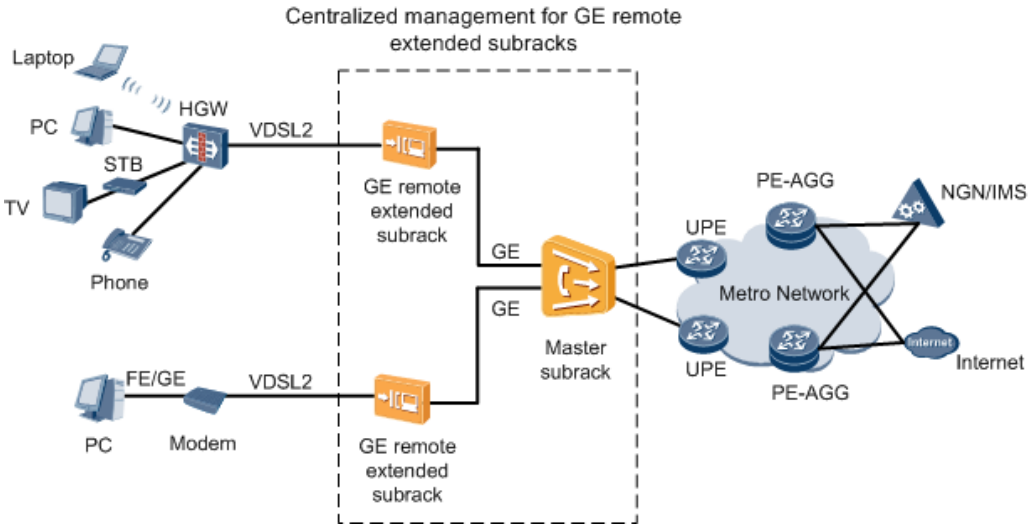
Copyright © Huawei Technologies Co., Ltd.

- When using traditional VDSL2 modems for user access:
  - For HSI service, users are provided with the HSI service through modems at their home. Dialup authentication is required because modems are Layer 2 devices. Each user has an independent account and is authenticated and managed on the BRAS.
  - For voice service, users are provided with the traditional telephone service by connecting telephones to the VDSL2 splitter.
- When using HGWs for user access:
  - The HGW is connected to the upstream extended subrack through VDSL2 ports, and provides the Internet access service through FE or Wi-Fi ports and the IPTV service through FE ports in the downstream direction.
  - The HGW has Layer 3 functions (such as PPPoE dialup and NAT), which enables multiple PCs of a family to access the Internet at the same time.
  - The STB connected to the HGW provides IPTV program preview and access functions.
  - The IAD embedded in the HGW provides one or several POTS ports, which provides access for multiple phones of a family at the same time.

Applicable master subrack: MA5600T, MA5603T (uses the SCUN board as the control board, and is cascaded to the GE remote extended subrack through the ETHB board.)

Applicable GE remote extended subrack: MA5623AR

Figure 11-12 Service networking diagram for GE remote extended subracks



11.4.2.2 Principle of Data Planning for GE Remote Extended Subrack

Data planning for GE remote extended subracks covers security data, QoS data, and data about the cascading between the master subrack and the extended subrack (including the reliability of uplink links on the extended subrack).

Copyright © Huawei Technologies Co., Ltd.

Data Plan for Cascading Between the Master Subrack and the GE Remote Extended Subrack (Including the Reliability of Uplink Links on the Extended Subrack)

Item	Solution
Extending port of the master subrack	Adding a GE remote extended subrack to a master subrack is like adding a service board to the master subrack. You can add a GE remote extended subrack in offline pre-deployment or automatic discovery mode. In offline pre-deployment mode, an extending port on the master subrack needs to be planned for adding the extended subrack. In automatic discovery mode, an extending port does not need to be planned, and the port where the extended subrack is automatically discovered is used as the extending port.
Extended subrack ID	The master subrack ID is always 0. After the GE remote extended subrack is introduced, the extended subrack ID starts from 1. Currently, a maximum of 32 extended subracks are supported. Therefore, the extended ID ranges from 1 to 32. In offline pre-deployment mode, an available subrack ID needs to be specified for the extended subrack to be added. In automatic discovery mode, the master subrack automatically allocates an available subrack ID to the extended subrack that is confirmed.
Reliability of uplink links on the extended subrack	The reliability of uplink links on the extended subrack can be enhanced using only Ethernet link aggregation, which is similar to Ethernet link aggregation of the master subrack in upstream transmission. When a GE remote extended subrack is used, pay attention to the following points: ● Link aggregation can be performed only on an ETHB extending board, instead of between boards and only manually, instead of using LACP. ● If aggregation is performed for uplink links on the extended subrack, the ETHB extending port in the aggregation group of the master subrack must be set as the master port in the aggregation group. The ETHB extending port refers to the extending port specified during the offline configuration of the extended subrack or the extended subrack port that is discovered automatically. The master port in the aggregation group of the extended subrack can be configured as required.

Plan security and QoS data based on the following items:

- **QoS data planning**
- **Internet service data planning**
- **(Optional) Vectoring data planning**
- **Voice service data planning** (VoIP services are provided by home gateways and therefore, only planning voice VLANs for home gateways is required for voice services. PSTN voice

Copyright © Huawei Technologies Co., Ltd.

services are transmitted to PSTN networks through the splitter and therefore, FTTx network data planning is not required for PSTN voice services.)

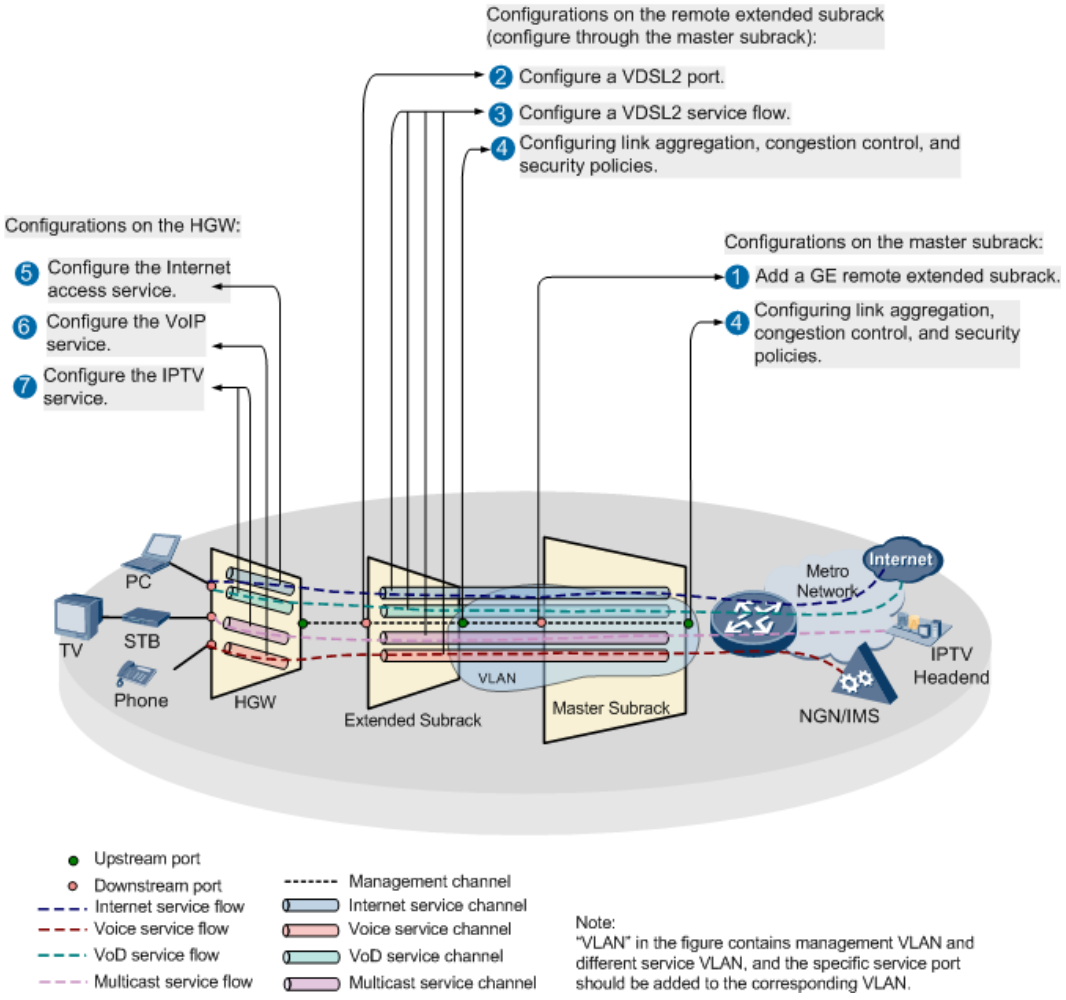
- **IPTV service data planning**
- **Security data planning**

11.4.2.3 Configuration Procedure for GE Remote Extended Subrack

Compared with a traditional network using VDSL2 modems to connect to users, the network using a GE remote extended subrack requires the **addition of a GE remote extended subrack**. The other service configuration process and methods are the same for the two networks and therefore are not described in this section. For details, see the *MA5600T Configuration Guide* or the *MA5603T Configuration Guide*. This section describes the service configuration process for the FTTB/FTTC+HGW networking (FTTB is the abbreviation for fiber to the building, FTTC for fiber to the curb, and HGW for home gateway).

Figure 11-13 shows the configuration roadmap for the FTTB/FTTC+HGW networking.

Figure 11-13 Configuration roadmap for the FTTB/FTTC+HGW networking (voice service provided through the HGW)



The following table describes the configuration steps.

Copyright © Huawei Technologies Co., Ltd.

Configuration Object	Step	Description
DSLAM (master subrack)	**Add a GE remote extended subrack.**	The operation of adding a GE remote extended subrack to the master subrack is the same as that of adding a service board to the master subrack. The GE remote extended subrack can be automatically discovered or deployed in offline mode. After the extended subrack is added, the master subrack manages it as a service board.
GE remote extended subrack (configured through the master subrack)	**Configure a VDSL2 port.**	Configure a VDSL2+ profile and bind it to the VDSL2 port. Then, activate the VDSL2 port for service transmission.
	Configure a VDSL2 service flow.	In HGW networking, a VDSL2 service flow is of the multi-service over multi-PVC type, which facilitates the management and maintenance of various services.
	(Optional) Configure vectoring.	The vectoring function enabled on a VDSL2 line can greatly cancel the far-end crosstalk (FEXT) on the line and increase the VDSL2 line rate.
	Configure link aggregation, congestion control, and security policies.	The global configuration of link aggregation and upstream queue scheduling based on priorities ensures service reliability. The global configuration of security policies ensures service security.
HGW	**Configure the Internet access service.**	Refer to service configurations on the HGW on the network where services are transmitted upstream through DSL lines.
	Configure the IPTV service.	
	Configure the voice service.	
GE remote extended subrack (configured through the master subrack) HGW	**Verify the configured services.**	PPPoE dialup, call, and multicast service emulation tests can be performed on the master subrack for the services on the GE remote extended subrack. This allows commissioning and configuration engineers to remotely verify services. VoD and HGW voice service do not support remote verification.

Copyright © Huawei Technologies Co., Ltd.

11.4.2.4 Adding GE Remote Extended Subracks

This topic describes how to add a GE remote extended subrack to the master subrack so that the master subrack can manage the extended subrack.

Data Plan

The following table lists the data plan for interconnection between the master subrack and extended subrack.

Item	Data	Remarks
Extending port of the master subrack	ETHB extending port: 0/3/0	Adding a GE remote extended subrack to a master subrack is like adding a service board to the master subrack. You can add a GE remote extended subrack in offline pre-deployment or automatic discovery mode. In offline pre-deployment mode (as in this example), an extending port on the master subrack needs to be planned for adding the extended subrack. In automatic discovery mode, an extending port does not need to be planned, and the port where the extended subrack is automatically discovered is used as the extending port.
Extended subrack ID	In offline pre-deployment mode, the extended subrack ID is 1.	The master subrack ID is always 0. After the GE remote extended subrack is introduced, the extended subrack ID starts from 1. Currently, a maximum of 32 extended subracks are supported. Therefore, the extended ID ranges from 1 to 32. In offline pre-deployment mode (as in this example), an available subrack ID needs to be specified for the extended subrack to be added. In automatic discovery mode, the master subrack automatically allocates an available subrack ID to the extended subrack that is confirmed.

Procedure

Step 1 Set the auto-negotiation function of the extending port to **enable**.

```
huawei(config-if-eth-0/3)#auto-neg all enable
```

Step 2 Set the working mode of the ETHB extending board to **extend**.

```
huawei(config-if-eth-0/3)#network-role extend
huawei(config-if-eth-0/3)#quit
```


Copyright © Huawei Technologies Co., Ltd.

NOTICE

An ETHB board resets if its working mode switches from **extend** to other modes or from other modes to **extend**.

Step 3 Add a remote extended subrack in offline mode.

```
huawei(config)#frame add 1 MA5623AR extend-port 0/3/0
```

----End

Follow-up Procedure

After being powered on, the extended subrack automatically communicates with the master subrack to complete registration, and enters the normal state. Then, the master subrack can manage the extended subrack.

NOTE

In automatic discovery mode, perform the following operations to add a remote extended subrack:

- Run the **display network-role** command to check whether the working mode of the ETHB board is **extend**
- If the working mode is not **extend**, run the **network-role** command to set the working mode to **extend**. Note that mode switching will reset the ETHB board.
- Run the **frame confirm** command to confirm the extended subrack. Then, the extended subrack enters the normal state.

11.4.2.5 Configuring VDSL2 User Ports

This topic describes how to activate VDSL2 ports and bind a VDSL2 profile to the ports for service transmission.

Data Plan

Data plan for VDSL2 user ports focuses on line parameters, such as spectrum profile, OSNR tolerance, and maximum interleave delay. The parameter plan for VDSL2 ports on a GE remote extended subrack is the same as that for VDSL2 ports on the master subrack. For details, see "Configuring VDSL2 Profiles" in *MA5600T/MA5603T Configuration Guide*.

Procedure

Step 1 Select a default VDSL2 profile ID, or configure a VDSL2 profile according to service requirements.

Step 2 Activate the VDSL2 user ports.

1. Run the **activate** command to activate the VDSL2 ports, and then bind a line profile (non-line-alarm profile) to the VDSL2 ports. Note that the format of the **activate** command varies with the VDSL2 modes (TR129, TI, or TR165).
2. Run the **alarm-config** command to bind a line alarm profile to the VDSL2 ports.

----End

Copyright © Huawei Technologies Co., Ltd.

11.4.2.6 Configuring VDSL2 Service Flows

This topic describes how to configure different service flows on GE remote extended subracks for different services so that service packets on HGWs can be forwarded at Layer 2 according to the planned VLAN and forwarding policies.

Data Plan

The following table lists the data plan for configuring service flows.

Service Type	VLAN Plan	Remarks
Internet access service	S-VLAN: 100; VLAN attribute: stacking C-VLAN: 1001–1002	The Internet access service use dual VLAN tags (S-VLAN+C-VLAN) to differentiate users. For details, refer to **11.2.3 Principle of Internet Access Service Data Plan**.
Voice service	S-VLAN: 200 C-VLAN: 200	The voice over IP (VoIP) service is a carrier-operating closed service. It primarily uses only S-VLAN tags which are transparently transmitted from a GE remote extended subrack to an HGW. For details, refer to **11.2.5 Principle of VoIP Service Data Plan**. **NOTE** VLAN planning is required only when HGWs provide all VoIP services. Service boards in the extended subrack do not process traditional public switched telephone network (PSTN) voice services that are transmitted through splitters. PSTN voice signals are transparently transmitted through the splitter upstream to PSTN networks.
VoD service	S-VLAN: 300 C-VLAN: 300	The PSPV mode is recommended for the video on demand (VoD) service because the service requires fewer VLANs. The voice over IP (VoIP) service is a carrier-operating closed service. It primarily uses only S-VLAN tags which are transparently transmitted from a GE remote extended subrack to an HGW. For details, refer to **11.2.6 Principle of IPTV Service Data Plan**.

Copyright © Huawei Technologies Co., Ltd.

Service Type	VLAN Plan	Remarks
Multicast service	MVLAN: 1000 IGMP version: IGMPv3 IGMP mode: IGMP proxy Multicast program library: 224.1.1.10–224.1.1.100 IP address of the multicast server: 10.10.10.10/24	The multicast service is a carrier-operating closed service and primarily uses only S-VLAN tags. For details, refer to **11.2.6 Principle of IPTV Service Data Plan**.

NOTE

C-VLANs in the preceding table are defined for remote extended subracks. That is, they are upstream VLANs or S-VLANs of HGWs.

Procedure

- Configure an Internet access service flow.
  1. Create an S-VLAN and add an upstream port to it.

     Create S-VLAN 100 with the stacking attribute and add upstream port 0/19/0 to the S-VLAN.

     ```
     huawei(config)#vlan 100 smart
     huawei(config)#vlan attrib 100 stacking
     huawei(config)#port vlan 100 0/19 0
     ```

  2. Configure a traffic profile.

     The 802.1p priority of the Internet access service is 0, and rate limitation is not required. To query existing traffic profiles, run the **display traffic table ip** command. In this example, the query result shows that traffic profile 6 meets the requirements, so no traffic profile needs to be configured.

     ```
     huawei(config)#display traffic table ip from-index 0
     ```

  3. Configure a service port to receive and transparently transmit the Internet access service from the HGW.

     Configure an Internet access service port with the user VLAN being 1001 or 1002. The HGW is connected to port 1/1/0 of the GE remote extended subrack. Upstream and downstream traffic is rate-limited using a line profile. A traffic profile (traffic profile 6 in this example) that does not limit rates is referenced.

     ```
     huawei(config)#service-port vlan 100 vdsl mode ptm 1/1/0 multi-service
     user-vlan 1001 rx-cttr 6 tx-cttr 6
     huawei(config)#service-port vlan 100 vdsl mode ptm 1/1/0 multi-service
     user-vlan 1002 rx-cttr 6 tx-cttr 6
     ```

- Configure a voice service flow.
  1. Create an S-VLAN and add an upstream port to it.

Copyright © Huawei Technologies Co., Ltd.

Create S-VLAN 200 with the common attribute and add upstream port 0/19/0 to the S-VLAN.

```
huawei(config)#vlan 200 smart
huawei(config)#port vlan 200 0/19 0
```

2. Configure a traffic profile.

   The 802.1p priority of the voice service is 5, and rate limitation is not required. To query existing traffic profiles, run the **display traffic table ip** command. In this example, the query result shows that no existing traffic profile meets the requirements, so a new traffic profile needs to be configured.

   Add traffic profile 9 and set *priority-policy* to **local-setting**. Then, traffic is scheduled based on the priority specified in the traffic profile.

   ```
   huawei(config)#traffic table ip index 9 cir off priority 5 priority-policy
   local-setting
   ```

3. Configure a service port to receive and transparently transmit the voice service from the HGW.

   Configure a service port with the user VLAN being 200. The HGW is connected to port 1/1/0 of the GE remote extended subrack. Upstream and downstream traffic is rate-limited using a line profile. A traffic profile (traffic profile 9 in this example) that does not limit rates is referenced.

   ```
   huawei(config)#service-port vlan 200 vdsl mode ptm 1/1/0 multi-service
   user-vlan 200 rx-cttr 9 tx-cttr 9
   ```

- Configure a VoD service port.

  1. Create an S-VLAN and add an upstream port to it.

     Create S-VLAN 300 with the common attribute and add upstream port 0/19/0 to the S-VLAN.

     ```
     huawei(config)#vlan 300 smart
     huawei(config)#port vlan 300 0/19 0
     ```

  2. Configure a VoD traffic profile.

     The 802.1p priority of the VoD service is 4, and rate limitation is not required. To query existing traffic profiles, run the **display traffic table ip** command. In this example, the query result shows that no existing traffic profile meets the requirements, so a new traffic profile needs to be configured.

     Add traffic profile 10 and set *priority-policy* to **local-setting**. Then, traffic is scheduled based on the priority specified in the traffic profile.

     ```
     huawei(config)#traffic table ip index 10 cir off priority 4 priority-
     policy local-Setting
     ```

  3. Configure a VoD service port.

     Configure a service port with the user VLAN being 300. The HGW is connected to port 1/1/0 of the GE remote extended subrack. Upstream and downstream traffic is rate-limited using a line profile. A traffic profile (traffic profile 10 in this example) that does not limit rates is referenced.

     ```
     huawei(config)#service-port vlan 300 vdsl mode ptm 1/1/0 multi-service
     user-vlan 300 rx-cttr 10 tx-cttr 10
     ```

- Configure a multicast service flow.

Copyright © Huawei Technologies Co., Ltd.

1. Create an S-VLAN and add an upstream port to it.

   Create S-VLAN 1000 with the common attribute and add upstream port 0/19/0 to the S-VLAN.

   ```
   huawei(config)#vlan 1000 smart
   huawei(config)#port vlan 1000 0/19 0
   ```

2. Create a multicast service port.

   Configure a service port with the user VLAN being 1000. The HGW is connected to port 1/1/0 of the GE remote extended subrack. Upstream and downstream traffic is rate-limited using a line profile. A traffic profile (traffic profile 10 in this example) that does not limit rates is referenced.

   ```
   huawei(config)#service-port vlan 1000 vdsl mode ptm 1/1/0 multi-service
   user-vlan 1000 rx-cttr 10 tx-cttr 10
   ```

3. Set the IGMP version.

   Set the IGMP version to IGMP v3.

   ```
   huawei(config)#multicast-vlan 1000
   huawei(config-mvlan1000)#igmp version v3
   ```

4. Set the IGMP mode.

   Set the IGMP mode to IGMP proxy.

   ```
   huawei(config-mvlan1000)#igmp mode proxy
     Are you sure to change IGMP mode?(y/n)[n]:y
   ```

5. Configure the multicast upstream port.

   Configure the IGMP upstream port as 0/19/0.

   ```
   huawei(config-mvlan1000)#igmp uplink-port 0/19/0
   ```

6. Configure multicast programs.

   Set the IP address of multicast programs to 224.1.1.10–224.1.1.100, and IP address of the multicast server to 10.10.10.10.

   ```
   huawei(config-mvlan1000)#igmp program add batch ip 224.1.1.10 to-ip
   224.1.1.100
    sourceip 10.10.10.10
   ```

----End

11.4.2.7 (Optional) Configuring Vectoring

Vectoring configurations on VDSL2 lines cancel the far-end crosstalk (FEXT) of VDSL2 lines to improve the line rate.

Context

For MA5623AR, when configuring vectoring, learn configuration item functions and configuration methods beforehand by referring to **Table 11-33**.

Copyright © Huawei Technologies Co., Ltd.

Table 11-33 Vectoring configuration items

Item	Function	Description	Commands
Global band plan	In the vectoring algorithm, the system requires that the upstream band and downstream band are separate from each other. Therefore, the band plan must be globally configured.	● The band plan can be globally configured only when vectoring is globally enabled. ● After vectoring is globally enabled, if the band plan configured for the line profile is incompatible with the band plan globally configured for vectoring and the upstream band plan and downstream band plan are not separate from each other, the port cannot be activated.	xdsl vectoring bandplan-type
Global vectoring configurations	Vectoring configurations take effect only when vectoring is globally enabled.	● Before enabling vectoring, globally configure the band plan. **NOTE** Services in a vectoring group port are interrupted when the vectoring function is enabled or disabled.	xdsl vectoring

Copyright © Huawei Technologies Co., Ltd.

Item	Function	Description	Commands
Vectoring profile	Configure the function of canceling the upstream and downstream crosstalk in the vectoring profile. After binding the configured vectoring profile to the ports, the system implements the vectoring algorithm on the ports in the vectoring group based on profile configurations.	By default, all ports are bound to vectoring profile 1. Default value: ● Upstream crosstalk cancelation: enable ● Downstream crosstalk cancelation: enable	Commands: ● Add a vectoring profile: xdsl vectoring-profile add ● Modify a vectoring profile: xdsl vectoring-profile modify ● Delete a vectoring profile: xdsl vectoring-profile delete ● Query a vectoring profile: display xdsl vectoring-profile ● Bind a vectoring profile to the port: vectoring-config (VDSL mode)
Policy for controlling frequent online and offline on ports	The Vectoring algorithm is executed every time a port in a Vectoring group goes online or offline. To prevent adverse impact on system functions due to long-term running Vectoring tasks caused by frequent online and offline on a port, set the policy for controlling frequent online and offline on ports based on site requirements.	By default, the policy for controlling frequent online and offline is set to limit.	xdsl frequently-retrain-control

Copyright © Huawei Technologies Co., Ltd.

Item	Function	Description	Commands
Vectoring crosstalk matrix	The vectoring crosstalk matrix refers to crosstalk on a port in a vectoring group from other ports in the same vectoring group.	Before querying information about the vectoring crosstalk matrix, ensure that the global vectoring function is enabled and the specified port is in a vectoring group and activated.	display xdsl vectoring crosstalk-coupling-matrix

Copyright © Huawei Technologies Co., Ltd.

Item	Function	Description	Commands
Policy for activating a legacy customer premises equipment (CPE)	A legacy CPE is a VDSL2 CPE (supporting G. 993.2, not G. 993.5) that does not support Vectoring. If such a CPE is activated in G.993.2 mode in the Vectoring system, the crosstalk impact on other lines cannot be canceled, causing the Vectoring system performance to deteriorate. To minimize the impact, set the activation policy of a legacy CPE based on site requirements.	By default, the policy for activating a legacy CPE is set to limit. ● **no-limit**: The Vectoring legacy CPE is activated in common VDSL2 mode (G.993.2 mode), or non-Vectoring mode, in which the Vectoring system performance is affected. This mode is used in the Vectoring initial phase when a large number of CPEs need to be upgraded or replaced and the Vectoring performance are not concerned. ● **limit**: The Vectoring legacy CPE is activated in common VDSL2 mode but the line PSD is automatically shaped so that the CPE can be activated at a low VDSL2 rate, preventing crosstalk on other lines. This mode is used in Vectoring medium phase when some CPEs have not been upgrade or replaced. ● **force-friendly-ds-limit-us**: **force friendly** is used in the downstream	xdsl vectoring legacy-cpe activate-policy

Copyright © Huawei Technologies Co., Ltd.

Item	Function	Description	Commands
		direction and PSD automatic shaping is used in the upstream direction. ● **force-friendly-ds-no-limit-us**: **force friendly** is used in the downstream direction and no restriction is used in the upstream direction. ● **block**: The Vectoring legacy CPE cannot be activated in common VDSL2 mode. This mode is used in Vectoring mature phase when its performance is concerned and unnecessary crosstalk must be prevented.	

Data Plan

The **Table 11-34** lists key parameters of vectoring configurations.

Table 11-34 Key parameters of vectoring configurations

Item	Data	Description
Global vectoring configurations	enable	-
Global band plan	● Band plan type: 998ade ● USO type: type-a	-
Policy for activating a legacy customer premises equipment (CPE)	no-limit	The policy for activating a vectoring legacy CPE is configured as **no-limit** at the initial stage of vectoring application.

Copyright © Huawei Technologies Co., Ltd.

Item	Data	Description
Policy for controlling frequent online and offline on ports	no-limit	-
Vectoring group	Group ID: 1	All ports are added to the default vectoring group 1.
Vectoring profile	Profile ID: 1 The upstream/ downstream crosstalk cancelation function in default Profile 1 are as follows: ● Upstream crosstalk cancelation: enable ● Downstream crosstalk cancelation: enable	-

Procedure

Step 1 Globally configure the band plan type.

```
huawei(config)#xdsl vectoring bandplan-type 998ade us0-type type-a
```

Step 2 Configure the vectoring profile as **huawei** and bind it to the VDSL2 port in the vectoring group.

```
huawei(config)#xdsl vectoring-profile add control enable enable name huawei
huawei(config)#interface vdsl 1/1
huawei(config-if-vdsl-1/1)#vectoring-config all profile-name huawei
huawei(config-if-vdsl-1/1)#quit
```

Step 3 Configure the policy for activating a vectoring legacy CPE.

```
huawei(config)#xdsl vectoring legacy-cpe activate-policy no-limit
```

Step 4 Configure the policy for controlling frequent online and offline on ports.

```
huawei(config)#xdsl frequent-retrain-control 1/1/0 control-policy no-limit
```

Step 5 Enable the global vectoring.

```
huawei(config)#xdsl vectoring enable
```

Step 6 Save the data.

```
huawei(config)#save
```

----End

11.4.2.8 Configuring Link Aggregation, Congestion Control, and Security Policies

This topic describes how to configure uplink aggregation and priority scheduling policies for upstream queues in global config mode to enhance service reliability, and configure security policies in global config mode to secure services.

Context

Link aggregation aggregates multiple upstream Ethernet ports into a group to increase the uplink bandwidth and improve service reliability. It is advisable to configure congestion control.

Copyright © Huawei Technologies Co., Ltd.

Congestion control queues packets from one port into multiple queues and schedules the packets based on queue priorities. It is advisable to configure congestion control.

Security policies involve system security, user security, and service security, securing services from different aspects.

NOTE

It is advisable to enable a required service security feature according to the service type. For details, see **11.2.7 Principle of Security Data Plan**.

Procedure

- Configure link aggregation.

  Configure upstream ports 0/19/0 and 0/19/1 of the master subrack as a link aggregation group (LAG). Each member port in the LAG is allocated packets based on the source MAC address, and works in LACP static aggregation mode.

  ```
  huawei(config)#link-aggregation 0/19 0-1 ingress workmode lacp-static
  ```

  Configure upstream ports 1/0/0 and 1/0/1 of the GE remote extended subrack as an LAG. Each member port in the LAG is allocated packets based on the source MAC address, and works in manual aggregation mode. Ports 1/0/0 and 1/0/1 are connected to ports 0/3/0 (extending port) and 0/3/1 respectively on the ETHB extending board of the master subrack.

  NOTICE

  Pay attention to the following when configuring link aggregation for GE remote extended subracks:

  - Only intra-ETHB extending board aggregation in manual aggregation mode is supported.
  - For the uplink aggregation configuration on the master subrack, the ETHB extending port (which is specified during the offline pre-deployment of an extended subrack or where an extended subrack is automatically discovered) must be configured as the master port of an LAG. However, the extended subrack has no requirements on the master port of an LAG.
  - Before adding/deleting a port to/from an LAG, if the port is connected to a peer device, run the **shutdown** command to deactivate the slave port of the LAG or remove the fiber from the slave port to prevent a loopback. (Note that ports on the ETHB board support the **shutdown** command, but upstream ports of the extended subrack do not.) After the LAG is configured, re-activate the port or reconnect the fiber to the slave port.

  ```
  huawei(config)#link-aggregation 1/0 0-1 egress-ingress
  huawei(config)#link-aggregation 0/3 0 0/3 1 egress-ingress
  ```

- Configure queue scheduling.

  According to "**11.2.2 Principle of QoS Data Plan**", all packets are scheduled in strict priority queue mode and mapped into different queues based on priorities.

  ```
  huawei(config)#queue-scheduler strict-priority
  huawei(config)#cos-queue-map cos0 0 cos4 4 cos5 5 cos6 6
  ```

- Configure system security.
  - Enable deny of service (DoS) anti-attack on the master subrack.

Copyright © Huawei Technologies Co., Ltd.

1. Run the **security anti-dos enable** command to globally enable DoS anti-attack.
2. Run the **security anti-dos control-packet policy** command to configure a protocol packet processing policy that will be used when a DoS attack occurs.
3. Run the **security anti-dos control-packet rate** command to configure the threshold for the rate of sending protocol packets to the CPU.

- Enable IP address anti-attack on the master subrack.

  Run the **security anti-ipattack enable** command to enable IP address anti-attack.

- Configure user security.
  - Enable MAC address anti-flapping on the master subrack.

    Run the **security anti-macduplicate enable** command to enable MAC address anti-flapping.
  - Enable MAC address anti-spoofing on the master subrack.
    1. In global config mode, run the **security anti-macspoofing enable** command to globally enable MAC address anti-spoofing.
    2. Enable MAC address anti-spoofing at VLAN level in global config mode or service profile mode:
       a. In global config mode, run the **security anti-macspoofing vlan** command to enable MAC address anti-spoofing.
       b. Perform the following operations to enable MAC address anti-spoofing in service profile mode:
          a. Run the **vlan service-profile** command to create a VLAN service profile.
          b. Run the **security anti-macspoofing enable** command to enable MAC address anti-spoofing at VLAN level.
          c. Run the **commit** command to make the profile configuration take effect.
          d. Run the **quit** command to quit the VLAN service profile mode.
          e. Run the **vlan bind service-profile** command to bind the created VLAN service profile to a VLAN.
    3. (Optional) Run the **security anti-macspoofing max-mac-count** command to set the maximum number of MAC addresses that can be bound to a service flow.
    4. (Optional) Run the **security anti-macspoofing exclude** command to configure the types of packets for which MAC address anti-spoofing does not take effect, such as Internet Group Management Protocol (IGMP) packets.
  - Enable IP address anti-spoofing on the master subrack.

    IP address anti-spoofing can be enabled or disabled at three levels: global, VLAN, and service port levels. This function takes effect only after it is enabled at the three levels. Among the three levels, IP address anti-spoofing is disabled only at the global level by default.
    1. In global config mode, run the **security anti-ipspoofing enable** command to enable IP address anti-spoofing at the global level.
    2. In VLAN service profile mode, run the **security anti-ipspoofing enable** command to enable IP address anti-spoofing at the VLAN level.

Copyright © Huawei Technologies Co., Ltd.

3. Run the **security anti-ipspoofing service-port** *serviceport-id* **enable** command to enable IP address anti-spoofing at the service port level.

- Configure service security.
  - Enable Dynamic Host Configuration Protocol (DHCP) Option 82 on the master subrack. This configuration is recommended for the DHCP-based Internet access service.

    DHCP Option 82 can be enabled or disabled at four levels: global, port, VLAN, and service port levels. This function takes effect only after it is enabled at the four levels. Among the four levels, DHCP Option 82 is disabled only at the global level by default.
    - The global level: In global config mode, run the **dhcp option82** command to enable DHCP Option 82 at the global level.

      When you run this command, select the **enable**, **forward**, or **rebuild** parameter based on site requirements. The three parameters can all enable DHCP Option 82 but provide different packet processing policies on the OLT. For details, see the **dhcp option82** command.
    - The port level: In global config mode, run the **dhcp option82 port** or **dhcp option82 board** command to enable DHCP Option 82 at the port level.
    - The VLAN level:
      1. In global config mode, run the **vlan service-profile** command to create a VLAN service profile.
      2. Run the **dhcp option82 enable** command to enable DHCP Option 82 at the VLAN level.
      3. Run the **commit** command to make the profile configuration take effect.
      4. Run the **quit** command to quit the VLAN service profile mode.
      5. Run the **vlan bind service-profile** command to bind the created VLAN service profile to a VLAN.
    - The service port level: In global config mode, run the **dhcp option82 service-port** command to enable DHCP Option 82 at the service port level.
  - Enable Policy Information Transfer Protocol (PITP) on the master subrack. This configuration is recommended for the PPPoE-based Internet access service.

    PITP can be enabled or disabled at four levels: global, port, VLAN, and service port levels. This function takes effect only after it is enabled at the four levels. Among the four levels, PITP is disabled only at the global level by default.
    - The global level: In global config mode, run the **pitp enable pmode**, **pitp forward pmode**, or **pitp rebuild pmode** command to enable PITP at the global level.

      In the preceding commands, the **enable**, **forward**, and **rebuild** parameters can all enable PITP but provide different packet processing policies on the OLT. Select one of them based on site requirements. For details, see the **pitp** command.
    - The port level: In global config mode, run the **pitp port** or **pitp board** command to enable PITP at the port level.
    - The VLAN level:
      1. In global config mode, run the **vlan service-profile** command to create a VLAN service profile.
      2. Run the **pitp enable** command to enable PITP at the VLAN level.

Copyright © Huawei Technologies Co., Ltd.

3. Run the **commit** command to make the profile configuration take effect.
4. Run the **quit** command to quit the VLAN service profile mode.
5. Run the **vlan bind service-profile** command to bind the created VLAN service profile to a VLAN.

- The service port level: In global config mode, run the **pitp service-port** command to enable PITP at the service port level.

----End

11.4.2.9 Configuring the Internet Access Service (on the HGW)

This topic describes how to configure the Internet access service for residential users on a home gateway (HGW) when the HGW is connected to an ONU upstream through a local area network (LAN) or in xDSL mode.

Context

Residential users generally access the Internet in Point-to-Point Protocol over Ethernet (PPPoE) dial-up mode. PPPoE dial-up can be performed on personal computers (PCs) or HGWs.

The configuration processes on HGWs of different models or in different appearances are similar. This topic describes how to configure the Internet access service on an HG239 that is connected to an ONU upstream through a LAN and on an HG527 that is connected to an ONU upstream in ADSL2+ mode.

Procedure

- Configure the Internet access service (on an HG239).
  1. Log in to the Web configuration window.
     a. Enter http://192.168.1.1/cu.html (default IP address) to the address bar of the Internet Explorer (IE) and press Enter.
     b. In the login dialog box, enter the user name and password of the administrator (the Internet service provider (ISP) provides the default user name and default password). Then, click **OK**.
  2. Set parameters for the Internet access service.

     Assume that ports LAN1 and LAN2 are Internet access ports for PCs.
     a. Choose **Network** > **Bandwidth Configuration** from the navigation tree.
     b. Create WAN connection 1 and set parameters based on the following table.

Parameter	Value
Bearing service	INTERNET

Copyright © Huawei Technologies Co., Ltd.

Parameter	Value
VLAN enabling	Enabled: Upstream packets contain VLAN tags. Disabled: Upstream packets do not contain VLAN tags. **NOTE** If **uservlan** is set to **untagged** when you configure a service flow for the Internet access service on the ONU, set this parameter to **Disabled**; otherwise, set it to **Enabled**.
VLANID [1-4094]	If **VLAN enabling** is set to **Enabled**, this parameter takes the value of **uservlan** that is specified when you configure a service flow for the Internet access service on the ONU.
Binding item	LAN1 and LAN2: PCs connected to ports LAN1 and LAN2 can simultaneously access the Internet.
Mode	Bridge: PCs access the Internet in PPPoE dial-up mode.

c. Click **OK**.

3. Restart the HGW.

   Choose **Management** > **Device Management** and click **Restarting the Device**.

- Configure the Internet access service (on an HG527).

  1. Log in to the Web configuration window.

     a. Enter http://192.168.1.1/cnc.html (default IP address) to the address bar of the IE and press Enter.

     b. In the login dialog box, enter the user name (default: admin) and password (default: admin) of the administrator. Then, click **OK**.

  2. Set parameters for the Internet access service.

     Assume that ports LAN1 and LAN2 are Internet access ports for PCs.

     a. Choose **Network** > **Bandwidth Configuration** from the navigation tree.

     b. Create WAN connection 1 and set parameters based on the following table.

Parameter	Value
Bearing service	INTERNET
Enabling	If this parameter is selected, WAN connection 1 is used.
VPI/VCI	Contact your carrier for the value ranges of VPIs and VCIs. Ensure that the VPI/VCI setting (for example, 0/35) on an HGW is consistent with that on the office to which the HGW is connected.
Binding item	LAN1 and LAN2: PCs connected to ports LAN1 and LAN2 can simultaneously access the Internet.
Mode	Bridge: PCs access the Internet in PPPoE dialup mode.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Value
Encapsulation mode	LLC

c. Click **OK**.

3. Restart the HGW.

   Choose **Management** > **Device Management** and click **Restarting the Device**.

----End

11.4.2.10 Configuring the IPTV Service (on the HGW)

This topic describes how to configure the IPTV service on the HGW that uses LAN or xDSL for upstream transmission. This configuration enables home subscribers to watch IPTV programs using STBs and TVs.

Context

HGWs have different models and appearances but their configuration procedures are similar. This topic uses the HG239 that uses LAN for upstream transmission and the HG527 that uses ADSL2+ for upstream transmission as examples.

Procedure

- Configure the IPTV service on the HG239.
  1. Log in to the Web configuration window.
     a. Enter http://192.168.1.1/cu.html (default IP address) to the address bar of the Internet Explorer (IE) and press Enter.
     b. In the login dialog box, enter the user name and password of the administrator (the Internet service provider (ISP) provides the default user name and default password). Then, click **OK**.
  2. Configure multicast parameters.

     This example assumes LAN 4 as an IPTV port.
     a. Choose **Network** > **Bandwidth Configuration** from the navigation tree.
     b. In the right pane, create LAN connection 2 for the IPTV service. Set the parameters as follows:

Parameter	Value
Bearing service	**OTHER**: The connection is used for the IPTV service.
VLAN enabling	**Enable** VLAN tags are added to upstream packets. **NOTE** When multicast service flows are created on the ONU, the value is **Disable** if **uservlan** is untagged and the value is **Enable** if **uservlan** is tagged.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Value
VLANID [1-4094]	Multicast VLAN ID corresponding to the user VLAN value for multicast service flows created on the ONU. In this example, set this parameter to 43.
Binding item	LAN4
Mode	Bridge
DHCP transparent transmission	Enable

c. Click **OK** to save the settings.

3. Restart the HGW.

   Choose **Management** > **Device Management** and click **Restarting the Device**.

- Configure the IPTV service on the HG527.

1. Log in to the Web configuration window.

   a. Enter http://192.168.1.1/cnc.html (default IP address) to the address bar of the IE and press Enter.

   b. In the login dialog box, enter the user name (default: admin) and password (default: admin) of the administrator. Then, click **OK**.

2. Configure multicast parameters.

   This example assumes LAN 4 as an IPTV port.

   a. Choose **Network** > **Bandwidth Configuration** from the navigation tree.

   b. In the right pane, create LAN connection 1 for dialup Internet access services. Set the parameters as follows:

Parameter	Value
Bearing service	**OTHER**: The connection is used for the IPTV service.
Enabling	The LAN connection is enabled when this check box is selected.
VLAN enabling	**Enable**: VLAN tags are added to upstream packets. **NOTE** When multicast service flows are created on the ONU, the value is **Disable** if **uservlan** is untagged and the value is **Enable** if **uservlan** is tagged.
VLANID [1-4094]	Multicast VLAN ID on the HGW when multicast service flows are created on the ONU. In this example, set this parameter to **43**.
VPI/VCI	Set the VPI/VCI to the same as that configured on the devices at the central office. In this example, set this parameter to **0/35**.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Value
Binding item	LAN4
Mode	Bridge
Encapsulation mode	LLC

c. Click **OK** to save the settings.

3. Restart the HGW.

   Choose **Management** > **Device Management** and click **Restarting the Device**.

----End

11.4.2.11 Configuring the VoIP Service (on the HGW)

This topic describes how to configure the voice service on HGWs that use LAN or xDSL for upstream transmission. This configuration enables home subscribers to enjoy the POTS service by using an analog telephone.

Context

HGWs have different models and appearances but their configuration procedures are similar. This topic uses the HG255 that uses LAN for upstream transmission and the HG555 that usesADSL2+ for upstream transmission as examples.

The IADs use SIP as the voice protocol.

Procedure

- Configure the VoIP service on the HG255.
  1. Log in to the Web configuration interface.
     a. Enter **http://192.168.1.1** (default IP address) in the address bar of the browser and press Enter.
     b. In the login window, enter the user name and password (the default value is provided by ISP) of the administrator and click **OK**.
  2. Configure parameters of the voice service.

     The configuration procedure is as follows:
     a. In the Web page, choose **Network** > **Bandwidth Configuration** from the navigation tree.
     b. Create WAN Connection 3 for the VoIP service and set the parameters as follows:

Parameter	Value
Bearing service	VoIP
Enabling status	Enable

Copyright © Huawei Technologies Co., Ltd.

Parameter	Value
VLAN mode	VLAN Transparent Transmission
VLAN ID	VLAN ID corresponding to the user VLAN value for voice service flows created on the ONU. In this example, set this parameter to 200.
802.1p	Enabled
Mode	Route: route mode
DHCP	Enabled
NAT	Enabled

c. Click **OK** to save the settings.

d. Choose **Appliciation** > **Broadband Phone Configuration** from the navigation tree. Configure the parameters as follows:

Parameter	Value
Address	Preferred IP address of the proxy server: 200.200.200.200
Port ID	Preferred signaling port ID of the proxy server: 5060
Enabling	Enabled
User number	When logging in to a VoIP account, you can set the user account to the user telephone number. In this example, set the user telephone number to 83110001.
User password	-

3. Restart the HGW.

   Choose **Management** > **Device Management** and click **Restarting the Device**.

- Configure the VoIP service (HG555)

  1. Log in to the Web configuration interface.

     a. Enter **http://192.168.1.1** (default IP address) in the address bar of the browser and press Enter.

     b. In the login window, enter the user name and password (the default value is provided by ISP) of the administrator and click **OK**.

  2. Configure parameters of the voice service.

     The configuration procedure is as follows:

     a. Click **Appliciation** > **Broadband Phone Configuration** from the navigation tree.

     b. Create WAN Connection 3 for the VoIP service and set the parameters as follows:

Copyright © Huawei Technologies Co., Ltd.

Parameter	Value
Bearing service	VoIP
Enabling status	Implement
VPI/VCI	Set the VPI/VCI to the same as that configured on the devices at the central office. In this example, set this parameter to 0/35.
VLAN mode	VLAN Transparent Transmission
VLAN ID	VLAN ID corresponding to the user VLAN value for voice service flows created on the ONU. In this example, set this parameter to 200.
802.1p	Enabled
Mode	Route mode
DHCP	Enabled
NAT	Enabled

c. Click OK.

d. Choose **Appliciation** > **Broadband Phone Configuration** from the navigation tree. Configure the parameters as follows:

Parameter	Value
Address	Preferred IP address of the proxy server: 200.200.200.200
Port ID	Preferred signaling port ID of the proxy server: 5060
Enabling	Enabled
User number	When logging in to a VoIP account, you can set the user account to the user telephone number. In this example, set the user telephone number to 83110001.
User password	-

3. Restart the HGW.

   Choose **Management** > **Device Management** and click **Restarting the Device**.

----End

11.4.2.12 Verifying Services

This topic describes how to verify services such as Internet access and IPTV services.

Copyright © Huawei Technologies Co., Ltd.

Prerequisites

The master subrack and upper-layer devices have been connected correctly, and the BRAS has been configured.

Context

The following table lists the remote verification methods for different services.

NOTE

The VoD service and voice service on HGWs do no support remote service verification.

Remote Verification Method	Function	Remarks
PPPoE dialup emulation	Emulates PPPoE user terminal to perform dialup and interact with the BRAS to verify the connectivity between the access device and BRAS.	● PPPoE dialup emulation requires a service flow which does not belong to a QinQ VLAN. ● A user name, password, and authentication mode must be configured on the BRAS for the PPPoE dialup emulation. ● A GE remote extended subrack supports a maximum of one PPPoE dialup emulation at the same time.
Multicast emulation	Emulates a multicast user going online and leads the program stream to an access device. You can check whether the multicast service is normal by checking the real-time traffic of the multicast program.	Multicast services configured in the dynamic controllable multicast mode do not support this function.

Data Plan

Item	Data	Remarks
PPPoE dialup emulation parameters	Referenced service flow ID: 101 Emulation timeout time: 10s	The user name, password, and authentication mode for the emulation test must be configured on the BRAS and must be the same as those planned for the BRAS.
Multicast emulation parameters	Multicast service flow ID: 401 MVLAN: 1000 IP address of the multicast program: 224.1.1.10	-

Copyright © Huawei Technologies Co., Ltd.

Procedure

- Verify the Internet access service using PPPoE dialup emulation.
  1. Start an emulation test by running the **simulate dhcp start** command.

```
huawei(config)#pppoe simulate start
  Command:
          pppoe simulate start
 Service-port(index<0-999>):101
 User Name(length<1,65>):user0
 User Password(length<0,16>):*******
 Authentication Mode:
 1. Chap  2. Pap [default 1]:1
 Overtime Time(5-60s)[default 5]:10
```

  2. Query the emulation test information by running the **display pppoe simulate info** command.

```
huawei(config)#display pppoe simulate info
  PPPoE simulate information is:
  ------------------------------------------------------------------
  Service-port:  101
  User name:     user0
  Current phase: -                     //*Emulation phase
  Result:        Success               //*Emulation result
  Start time:    2011-11-16 15:41:29+08:00
  End time:      2011-11-16 15:41:34+08:00
  Session ID:    591
  User IP:       192.168.50.2
  Gateway IP:    192.168.50.254
  ------------------------------------------------------------------
```

  3. Terminate the emulation test by running the **simulate dhcp start** command.

```
huawei(config)#pppoe simulate stop
```

- Verify the multicast service using multicast emulation.
  1. Run the **igmp static-join** command to order a multicast program by emulating a multicast user.

```
huawei(config)#btv
huawei(config-btv)#igmp static-join service-port 401 ip 224.1.1.10 vlan
1000
```

  2. Run the **display igmp use** command to query the status of the multicast user.

```
huawei(config-btv)#display igmp user service-port 401
  User                       : 0/3/1 //*Use an ETH port as an example.
  State                      : online
  Authentication             : no-auth
  Quick leave                : MAC-based
  IGMP flow ID               : 0
  Video flow ID              : 0
  Log switch                 : enable
  Bind profiles              : -
  IGMP version               : IGMP v3
  Available programs         : 91
  Global Leave               : disable
  User MaxBandWidth          : no-limit
  Used bandwidth(kbps)       : 5000
  The percentage of used
  bandwidth to port rate(%)  : -
  Total video bandwidth      : -
  Mcast video bandwidth      : -
  Active program list

  ------------------------------------------------------------------------
```


Copyright © Huawei Technologies Co., Ltd.

```
--
  Program name     VLAN  IP/MAC          State           Start-time

------------------------------------------------------------------------
--
  program1         1000  224.1.1.10      watching        2011-07-13
                                                         14:41:18

------------------------------------------------------------------------
--
  Total: 1
```

3. Run the **display multicast flow-statistic** command to query the real-time traffic of the multicast program.

```
huawei(config-btv)#display multicast flow-statistic ip 224.1.1.10 vlan
1000
  Command is being executed, please wait...
  Multicast flow statistic result: 360(kbps)
```

- Verify the VoD service.
  1. Run the **display mac-address service-port** command to check whether the MAC addresses of VoD subscribers are learned. If yes, the VoD service is reachable.
- Verify the voice service.
  1. Log in to the HGW management web page.
  2. Choose **Status** > **Broadband VoIP Information** to query the service registration status and phone number.

     Expected service registration status: Register successfully.

----End

Copyright © Huawei Technologies Co., Ltd.

12 FTTO Configuration(SOHO and SME)

About This Chapter

This chapter describes the configurations of the following services for small office and home office (SOHO) users and small- and medium-sized enterprises (SMEs) in fiber to the office (FTTO) scenarios: services of Internet access through cables, services of Internet access through wireless fidelity (Wi-Fi), VoIP services, fax services, point of sale (POS) services, multicast services, and private line services.

Context

FTTO is positioned for SOHO users, SMEs, and enterprises. This chapter provides service configurations only for SOHO users and SMEs. For details about service configurations for enterprises, see **13 FTTO Configuration (Large-sized Enterprise Access)**.

12.1 Overview of FTTO Services (SOHO and SME)
This section describes small office and home office (SOHO) and small- and medium-sized enterprise (SME) services in fiber to the office (FTTO) scenarios from the aspect of basic concepts, networking scenarios, typical configurations, and optical network unit (ONU) capability set. This information provides a basis for SOHO and SME service configurations in FTTO scenarios.

12.2 Principles of Planning Data for FTTO Services (SOHO and SME)
This section describes the principles of planning data for small office and home office (SOHO) users and small- and medium-sized enterprises (SMEs) in fiber to the office (FTTO) scenarios, from the aspect of security, device management, quality of service (QoS), and services. The data of all the examples involved in this section is planned following the principles.

12.3 SOHO Service Configuration (GPON)
This section describes Internet access, voice, and video service configurations for small office and home office (SOHO) users in GPON access mode in fiber to the office (FTTO) scenarios.

12.4 SME Service Configuration (GPON)
This section describes Internet access, voice, video, and Layer 2 bridging service configurations for small- and medium-sized enterprises (SMEs) in GPON access mode in fiber to the office (FTTO) scenarios.

Copyright © Huawei Technologies Co., Ltd.

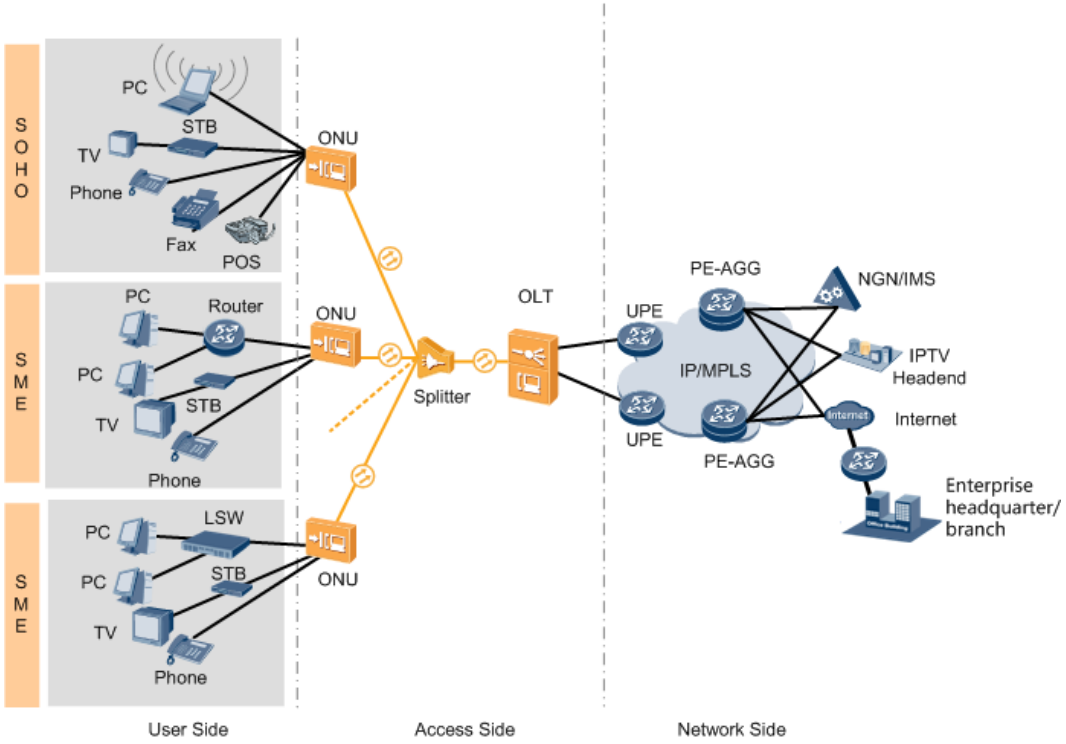
12.1 Overview of FTTO Services (SOHO and SME)

This section describes small office and home office (SOHO) and small- and medium-sized enterprise (SME) services in fiber to the office (FTTO) scenarios from the aspect of basic concepts, networking scenarios, typical configurations, and optical network unit (ONU) capability set. This information provides a basis for SOHO and SME service configurations in FTTO scenarios.

12.1.1 Basic Concept

FTTB and FTTC solutions involve many concepts. This topic describes concepts involved in FTTB and FTTC solutions from user side to network side based on the following integrated FTTB and FTTC network diagram.

Integrated FTTB and FTTC Network Diagram



Scenario

Concept	Description
Small office home office (SOHO)	SOHO is positioned for miniature enterprises, such as home offices, shops, and markets.
Small- and medium-sized enterprise (SME)	An SME contains 10-300 personnel. SME is positioned for small- and medium-sized enterprises, campuses, and net bars.

Copyright © Huawei Technologies Co., Ltd.

User Side

Concept	Introduction
VoD	VoD is known as interactive video on demand. Users can choose their desired programs from the VoD program database. When watching programs, users can perform operations such as pause, fast forward, fast rewind, and locate.
Multicast	Multicast, or broadband TV (BTV) is similar to traditional wired broadcasting or television satellite broadcasting. Users have the same experience in watching BTV programs and traditional television programs. Unlike the traditional television, the IPTV system encodes audio signals into media streams and multicasts the media streams over an IP network to user terminals.
Fax	A communication tool widely used in enterprises and institutions to transmit digital text and images through phone lines.
Point of sale (POS)	A terminal supporting multiple functions. After being installed in a promissory shop or designated network of a credit card and accessing the network, the POS machine implements speedy, convenient, and reliable automatic electronic funds transfer. The POS machine supports consumption, advance payment, balance inquiry, and transfer.
Wireless fidelity (Wi-Fi)	A short-distance wireless transmission technology, which supports wireless signals for Internet access within hundreds of feet.

Access Side

Concept	Introduction
PON	A passive optical network (PON) uses a point-to-multipoint (P2MP) network architecture. A PON network consists of three parts: optical line terminal (OLT), optical distribution network (ODN), and optical network units (ONUs). A PON network uses optical fibers for data transmission, supports more users with less optical fiber resources, and provides a higher access rate.
ODN	The ODN is composed of passive optical components, such as optical fibers and one or more passive optical splitters. The ODN provides highly reliable optical channels between the OLT and ONUs.
OLT	The OLT is an aggregation device located at the central office (CO), which terminates PON protocols. OLTs in this document are MA5600T/MA5603T/MA5608T.
ONU	ONUs are located on the user side, providing various types of ports for connecting to user terminals. The ONUs communicate with the OLT through a passive ODN.

Copyright © Huawei Technologies Co., Ltd.

Concept	Introduction
Split Ratio	Split ratio is the ratio of dividing a downstream optical signal into sub-signals in the PON system. Greater optical ratio requires more power to support physical distances.

Network Side

Concept	Introduction
U-PE	User-end provider edges (U-PEs) are routing devices directly connected to customer edges (UEs). U-PEs support routing and MPLS encapsulation. If a U-PE is connected to multiple CEs and possesses the basic bridging function, data frame forwarding only needs to be performed on the U-PE. This reduces the load of the S-PE.
PE-AGG	Aggregation provider edge (PE-AGG) routers provide aggregation and route forwarding functions for access equipment. Compared with U-PEs, PE-AGGs features higher performance, fewer interfaces, and higher switching rates.
NGN/IMS	A next generation network (NGN) is a network that uses softswitches as its core and uses open and standardized architectures to provide abundant services such as VoIP, video, and data. The IP multimedia subsystem (IMS) uses SIP signaling as its call control signaling to provide services such as VoIP, data, and multimedia services. **NOTE** NGN/IMS in this document refers to softswitches that support H.248 and SIP.
IPTV head end	The IPTV head end system functions as the contents preparation platform in the IPTV system. It provides functions such as signal receipt, media format conversion, and media material management.

12.1.2 Networking Scenario and Hardware Configurations

This section describes the typical networking scenarios for small office and home office (SOHO) users and small- and medium-sized enterprises (SMEs) in GPON access mode in fiber to the office (FTTO) scenarios, as well as the typical hardware configurations of optical line terminals (OLTs) and optical network units (ONUs).

Copyright © Huawei Technologies Co., Ltd.

Typical Networking Scenarios and Hardware Configurations

Networking Scenario	Description	Typical OLT Configuration	ONU Device
FTTO SOHO networking	● ONUs are deployed for shops and markets. ● ONUs provide GE and POTS ports. Through the ports, the ONUs provide the following services for users: Internet access through cables, Internet access through wireless fidelity (Wi-Fi), broadband TV (BTV), VoD, VoIP, fax, and point of sale (POS).	SCUN+GPBD/ GPBH/GPFD +GICK/X2CS	MA5671, MA5675, and MA5675M
FTTO SME bridging networking	● In bridging mode, ONUs connect to an enterprise router through GE ports and provide the Internet access and VoD services for the users connected to the enterprise router. ● ONUs provide GE/FE and POTS ports. Through the ports, the ONUs provide the BTV and VoIP services for users.		MA5671, MA5672M, and MA5612
FTTO SME gateway networking	● In gateway mode, ONUs connect to an enterprise LAN switch through GE ports and provide the Internet access and VoD services for the users connected to the enterprise LAN switch. ● ONUs provide GE/FE and POTS ports. Through the ports, the ONUs provide the BTV and VoIP services for users.		MA5671, MA5672M, and MA5612

Copyright © Huawei Technologies Co., Ltd.

Networking Scenario	Description	Typical OLT Configuration	ONU Device
FTTO SME Layer 2 bridging networking	ONUs, deployed at enterprise branches, provide GE or FE ports. Through the ports, the ONUs receive and converge enterprise Ethernet services and transmit the services upstream to an OLT. This implements the communication between enterprise branches.		MA5671, MA5672M, MA5612, and MA5694

NOTE

For details about the SME private line service in FTTO scenarios, see **13 FTTO Configuration (Large-sized Enterprise Access)**.

12.1.3 ONU Capability Sets

This topic describes the hardware capabilities, features, and positioning of ONUs in SOHO and SME networks.

ONU Capability Sets

Table 12-1 shows the ONU capability sets provided.

Table 12-1 ONU capability sets

ONU Name	ONU Type	Uplink Port	User Port	ONU Version Supported	Feature and Positioning
MA5671	Gateway type	Provides a GPON port.	Provides 4 GE ports.	V800R313C00	Used in SOHO and SME scenarios.
MA5672M	Bridging and voice type	Provides a GPON port.	Provides 4 GE ports+8 POTS ports.	V800R313C00	Used in SME scenarios.
MA5675	Gateway type	Provides a GPON port.	Provides 4 GE ports+4 POTS ports+Wi-Fi access.	V800R313C00	Used in SOHO scenarios.
MA5675M	Gateway type	Provides a GPON port.	Provides 4 GE electrical ports+8 POTS ports +Wi-Fi access.	V800R313C00	Used in SOHO scenarios.

Copyright © Huawei Technologies Co., Ltd.

ONU Name	ONU Type	Uplink Port	User Port	ONU Version Supported	Feature and Positioning
MA5612	Gateway type	Provides two ports supporting autonegotiation between GPON, and GE.	For the bottom plate with POTS ports: ● Provides 2 GE electrical ports+6 FE electrical ports+48 POTS ports+ (optional)1 RF port when two ASNB boards are configured. ● Provides 2 GE electrical ports+22 FE electrical ports +16 POTS ports+ (optional)1 RF port when two EIUC boards are configured. ● Provides 2 GE electrical ports+6 FE electrical ports+16 E1/T1 ports+16 POTS ports+ (optional)1 RF interface when two E81A boards are configured. For the bottom plate without POTS ports: ● Provides 2 GE electrical ports+6 FE electrical ports+32 POTS ports when two ASNB boards are configured. ● Provides 2 GE electrical ports+22 FE electrical ports when two EIUC boards are configured. ● Provides 2 GE electrical ports+6 FE	V800R308C00 V800R308C01 V800R310C00 V800R311C00 V800R312C00	Used in SME scenarios.

Copyright © Huawei Technologies Co., Ltd.

ONU Name	ONU Type	Uplink Port	User Port	ONU Version Supported	Feature and Positioning
			electrical ports+16 E1/T1 ports when two E81A boards are configured.		
MA5694	Gateway type	Provides two ports supporting autonegotiation between GPON, and GE.	Provides 4 GE electrical ports (The ports are alternatively GE2 and GE3 electrical ports, or GE2 and GE3 optical ports.)	V800R313C00	Used in SME scenarios.

12.2 Principles of Planning Data for FTTO Services (SOHO and SME)

This section describes the principles of planning data for small office and home office (SOHO) users and small- and medium-sized enterprises (SMEs) in fiber to the office (FTTO) scenarios, from the aspect of security, device management, quality of service (QoS), and services. The data of all the examples involved in this section is planned following the principles.

NOTE

The principles of planning only the Internet access, voice, and multicast services are described. For details about the principles of planning the enterprise Layer 2 bridging service, see **13.2 Principle of Planning Data for Enterprise Access Service**.

12.2.1 Principles of Planing Device Management Data

The device management plan includes the channel management plan and the IP address plan.

Device Management Data Plan

Plan	Device/Service	Description
Management channel	OLT	Use a single-tagged VLAN as the device management VLAN of the OLT. All other devices in the network use single-tagged VLANs as the device management VLAN.

Copyright © Huawei Technologies Co., Ltd.

Plan	Device/Service	Description
	ONU/Router	Use a single-tagged S-VLAN as the management VLAN of the router that is managed. Set an S-VLAN for an entire network, an OLT, a PON board or a PON port for identifying services and physical locations. It is recommended that you set different router management VLANs for the OLTs connected to one SR to avoid an excessively large broadcast domain of the SR and convergence switch.
IP address plan (bridging + router networking)	Internet access service	As a Dynamic Host Configuration Protocol (DHCP) client, the router obtains a public IP address through PPPoE dialup. As a DHCP server, the router assigns private IP addresses to PCs that access the Internet through network cables or Wi-Fi. After Network Address Translation (NAT), all the PCs connected to the router use a public IP address to access the Internet. The ONU transparently transmits service packets.
	IPTV service	The router is configured with a bridging WAN port. The STB obtains a public IP address through DHCP. The router and the ONU transparently transmit service packets.
	VoIP service	As a DHCP client, the router obtains a public IP address through DHCP, or the ACS allocates a static IP address to the router through TR069. The voice signaling streams and the media streams of multiple POTS ports share the IP address. Media streams can be distinguished by different ports. The ONU transparently transmits service packets.
	TR069 management (optional)	As a DHCP client, the router obtains a public IP address through DHCP. The router connects to the TR069 server (ACS). The ONU transparently transmits service packets.
IP address plan (gateway networking)	Internet access service	As a DHCP client, the ONU obtains a public IP address through PPPoE dialup. As a DHCP server, the ONU allocates private network IP addresses to PCs that access the Internet through the network cables or Wi-Fi. After NAT, all the PCs connected to the router use the public IP address to access the Internet.

Copyright © Huawei Technologies Co., Ltd.

Plan	Device/Service	Description
	IPTV service	As a DHCP client, the ONU obtains a public network IP address through DHCP. As a DHCP server, the ONU allocates private IP addresses to STBs. After NAT, all the STBs connected to the ONU use a public IP address to order programs.
	VoIP service	As a DHCP client, the ONU obtains a public IP address through DHCP, or the NMS allocates an IP address to the ONU through a configuration file, or the ACS allocates a static IP address to the ONU through TR069. The voice signaling streams and the media streams of multiple POTS ports share the IP address. Media streams can be distinguished by different ports.
	TR069 management	In TR069-based management, maintenance and service provisioning, the ONU, functioning as a DHCP client, obtains a public network IP address through DHCP and connects to the TR069 server (ACS).

12.2.2 Principle of QoS Planning

The QoS planning is an E2E planning, and it can be divided into following policies: traffic classification, marking, and scheduling policy; and traffic monitoring and DBA policy.

Traffic Classification, Marking, and Scheduling Policy

Service Type	802.1p Priority	Queue Scheduling Method	OLT Queue ID (8 Queues)	ONU Queue.ID	
				When Eight Queues Are Supported	When Four Queues Are Supported
Management service	6	PQ	6	6	3
VoIP service	5	PQ	5	5	2
IPTV service	4	PQ	4	4	2
Internet access service	0	PQ	0	0	0

Copyright © Huawei Technologies Co., Ltd.

Note: The service priorities in this table are the recommended values. The service priorities are arranged according to the operators's actual plan.

Traffic Monitoring and DBA Policy

Items	Management service	Internet access service	VoIP service	IPTV service
GEM port	11 [Remark 1]	12	13	14
TCONT	All services share a T-CONT.			
DBA type	Type 3 (DBA profile: assured bandwidth + maximum bandwidth. Users are allowed to preempt the bandwidth on condition that the users' assured bandwidth is guaranteed. However, the total bandwidth cannot exceed the maximum bandwidth.)			
DBA bandwidth planning	Configure the DBA bandwidth according to the user's bandwidth package. The assured bandwidth is the maximum bandwidth required by management packets, VoIP, and IPTV upstream packets. The maximum bandwidth is larger than or equal to the maximum bandwidth that users apply.			
Rate limit on OLT downstream	No rate limit	Configure rate limit by a traffic profile as required. [Remark 2]	No rate limit	No rate limit
Rate limit on ONU upstream port	No rate restriction			
Rate limit on ONU downstream port	No rate restriction			

Remark 1: GEM port value depends on the planning of the service provider, but in principle, use different GEM ports for different services.

Remark 2: **Table 12-2** shows the reference service bandwidth of each service for each user.

Copyright © Huawei Technologies Co., Ltd.

Table 12-2 Reference service bandwidth of each service for each user

Service Type	Upstream Bandwidth	Downstream Bandwidth	Bandwidth Description
Internet access service	Determined based on the service tariff package.	Determined based on the service tariff package.	Available bandwidth or Internet access service = Committed bandwidth of the service tariff package - VoIP bandwidth - IPTV bandwidth
VoIP service	200 kbit/s	200 kbit/s	The upstream bandwidth and the downstream bandwidth of VoIP service are symmetrical. The actual bandwidth is related to the coding format. This bandwidth is calculated for two POTS ports.
IPTV service (standard definition program)	/	2.5 Mbit/s per channel	IPTV service mainly occupies the downstream bandwidth. The actual bandwidth depends on the coding format, the picture in picture information, 10% bandwidth burst traffic, and the number of programs that can be concurrently watched by one user (in the case of multiple STBs). The upstream bandwidth is mainly used for transmitting IGMP packets, which requires little bandwidth. Therefore, the bandwidth occupied by IGMP packets can be neglected.
IPTV service (high definition program)	/	9.7 Mbit/s per channel	

Note:

- The rate restriction on the BRAS or SR is recommended. OLTs and ONUs do not restrict the rate for service streams.
- If BRAS does not support rate restriction, OLTs can restrict the rate for service streams through the traffic profile.
- Different service packets on the ONU are distinguished by different VLAN IDs. The service packets are mapped to GEM ports based on VLAN IDs so that different service packets are transmitted to different GEM ports. Each GEM port (each service) corresponds to a T-CONT or all GEM ports share a T-CONT.

Copyright © Huawei Technologies Co., Ltd.

- The sum of the assured bandwidth of all ONUs connected to a PON port and the fixed bandwidth of OMCI management channel is less than the GPON upstream bandwidth. Some bandwidth must be reserved for the future service expansion.

12.2.3 Principle of Internet Access Service Data Plan

The Internet access service plan mainly includes the plan of the VLAN and VLAN translation policy in different network scenarios.

VLAN and VLAN Translation policy.

Application Scenario	VLAN Plan	VLAN Translation Policy
Bridging ONU + Router	Double-tagged VLAN	ONU: The upstream packets sent from the Router carry user-VLANs and the ONU transparently transmits them. OLT: The OLT translates the U-VLAN to S-VLAN+C-VLAN.
Gateway ONU	Double-tagged VLAN	ONU: ONUs configure the VLAN and add the same C-VLAN tag to packets. All ONUs are in the same C-VLAN. OLT: The OLT performs VLAN translation: C<->S+C'. The C'-VLAN of every ONU differs from each other.

Note:

- UserVLAN: VLAN carried by upstream packets of user-side devices, U for short.
- C-VLAN: VLAN added based on the ONU port. For details, see the description of the Double-tagged VLAN S+C.
- Double-tagged VLAN S+C: C indicates the inner VLAN (C-VLAN) and S indicates the outer VLAN (S-VLAN).
- Double-layer VLAN S+C': C' indicates the translated inner VLAN (C'-VLAN) and S indicates the outer VLAN (SVLAN).
- Single-tagged S-VLAN: Single-tagged VLAN marked or translated by the OLT. It is generally used in a single-tagged VLAN translation scenario.
- C<->S+C': Bidirectional VLAN translation: translates the inner C-VLAN and then adds one outer S-VLAN.
- C<->S+C: Bidirectional VLAN translation: maintains the inner C-VLAN and adds one outer S-VLAN.

Copyright © Huawei Technologies Co., Ltd.

NOTE

- To ensure traceability of users and finer-grained QoS control and management of users and services, plan per user per service per VLAN (PUPSPV) for the Internet access service. Considering OLT capacity and VLAN scalability, use dual VLANs (S-VLAN+C-VLAN) on the OLT to differentiate users for the Internet access service.
- The outer S-VLAN, which identifies services and physical location, can be allocated based on the OLT, PON board, or PON port. The inner C-VLAN identifies users. User C-VLANs must be unique in one S-VLAN.
- It is recommended that you use stacking VLANs as S-VLANs so that security features, such as PPPoE+/opton82, and anti MAC attacks and anti spoofing spoofing can be easily deployed.
- The 802.1q in 802.1q (QinQ) VLAN is used in the enterprise private line scenario, such as (TLS). The device transparently transmits packets. It is not recommended that you use QinQ VLANs as S-VLANs for the triple play services of residential users.

12.2.4 Principles of Planning Voice Service Data

The voice service plan mainly includes the plan of the VLAN and VLAN translation policy in different network scenario, and the plan of voice protocol.

VLAN and VLAN Translation Policy.

Usage Scenario	VLAN Plan	VLAN Translation Policy
Bridging ONU +router	Single-tagged VLAN	ONU: Provide the VoIP service through the ONU. Configure the service VLAN (S-VLAN) tag in a unified manner. OLT: The OLT transparently transmits S-VLAN tags.
	Double-tagged VLAN	ONU: Provide the VoIP service through the ONU. Configure the customer VLAN (C-VLAN) tag in a unified manner. The C-VLAN tag identifies the VoIP service. OLT: The OLT adds an S-VLAN tag to a C-VLAN tag and supports the switching between the C-VLAN tag and the S-VLAN+C-VLAN tag.
Gateway ONU	Single-tagged VLAN	ONU: Configure a VLAN for all ONUs and add the same C-VLAN tag to packets. All ONUs are in the same C-VLAN. OLT: The OLT transparently transmits VLAN tags (the C-VLAN is the same as the planned S-VLAN).

Copyright © Huawei Technologies Co., Ltd.

Usage Scenario	VLAN Plan	VLAN Translation Policy
	Single-tagged VLAN	ONU: Configure a VLAN for all ONUs and add the same C-VLAN tag to packets. All ONUs are in the same C-VLAN. OLT: The OLT switches between the C-VLAN tag and the S-VLAN tag (the C-VLAN is different from the planned S-VLAN).

Note:

- UserVLAN: VLAN carried by upstream packets of user-side devices, U for short.
- C-VLAN: VLAN added based on the ONU port. For details, see the description of the Double-tagged VLAN S+C.
- Double-tagged VLAN S+C: C indicates the inner VLAN (C-VLAN) and S indicates the outer VLAN (S-VLAN).
- Double-layer VLAN S+C': C' indicates the translated inner VLAN (C'-VLAN) and S indicates the outer VLAN (SVLAN).
- Single-tagged S-VLAN: Single-tagged VLAN marked or translated by the OLT. It is generally used in a single-tagged VLAN translation scenario.
- C<->S+C': Bidirectional VLAN translation: translates the inner C-VLAN and then adds one outer S-VLAN.
- C<->S+C: Bidirectional VLAN translation: maintains the inner C-VLAN and adds one outer S-VLAN.

NOTE

- The VoIP service is a closed service self-operated by carriers. The single-tagged S-VLAN is the mainstream application and is recommended.
- When the planned VLAN is single-tagged VLAN, the S-VLAN can identify services and physical locations based on an OLT device, a PON board or a PON port. It is recommended that you set different voice VLANs for the OLTs connected to one VoIP SR to avoid an excessively large broadcast domain of the SR and convergence switch.
- When the planned VLAN is S-VLAN+C-VLAN, the outer S-VLAN can identify services and physical locations based on an OLT device, a PON board or a PON port. The inner C-VLAN is used to identify services (the fixed value) and users.

VoIP Data Plan Based on H. 248 or SIP

Item			Description
MG interface/ SIP interface data	Media and signaling parameters	Media and signaling upstream VLANs	Upstream VLANs of the VoIP service

Copyright © Huawei Technologies Co., Ltd.

Item			Description
NOTE must be consistent with the data on the MGC/IMS core network devices.		Media and signaling upstream port	Upstream ports of the VoIP service
		Media IP addresses and signaling IP addresses	Supports separating media from signaling.
		Default gateway IP address.	The next hop IP address from an ONU/HGW to an MGC/IMS.
	MG interface/SIP interface ID		None
	Signaling port ID		Select a transmission mode according to the requirement on the MGC/IMS side.
	IP address of active MGC (H.248)/IP address of active IMS device (SIP)		If the dual homing is not configured, only one MGC parameter needs to be configured. If the dual homing is configured, the IP address and port ID of the standby MGC need to be configured.
	Port ID of active MGC (H248)/ port ID of active IMS device (SIP)		
	Coding		Select the coding method according to the requirement on the MGC/IMS side. Generally, the text coding method is adopted.
	Transmission mode		Select a transmission mode according to the requirement on the MGC/IMS side. Generally, the UDP transmission mode is adopted.
	Home domain (SIP)		None
	Profile index		None
	The version of H248 protocol that MG starts to negotiate		V1, V2 or V3 (by default). The interface may fail to be registered because some softswitches do not support V3.
Voice port data	Phone number		For H248 protocol: The phone numbers allocated by the MGC need to be determined, and the paging numbers for users' emergency standalone need to be planned if the emergency standalone function is provided. For SIP protocol: The phone number that the IMS core network device allocates to the user must be configured.

Copyright © Huawei Technologies Co., Ltd.

Item		Description
	Terminal ID (H248)	If the TID template with which the POTS user is bound does not support terminal layering, this parameter needs to be configured.
	User priority	According to the service requirements, user priorities must be specified. The user priorities include the following: ● cat1: government1 (category 1 government users) ● cat2: government2 (category 2 government users) ● cat3: common (common users)
	User type	According to the service requirements, user type needs to be specified. The user type includes the following: ● DEL: direct exchange lines (default) ● ECPBX: earth calling PBX ● LCPBX: loop calling PBX ● PayPhone: pay phone
Common parameter	system parameter	The system parameters including the overseas version flag and message waiting indication (MWI) mode need to be configured according to the local standard to ensure that the response of the user terminal complies with the local standard.
	Overseas parameters	The attributes such as the upper and lower thresholds of the flash-hooking duration need to be configured according to the local standards to ensure that the response of the user terminal complies with the local standards.
	POTS port attributes	If the POTS port needs to support the polarity reversal accounting, the POTS port needs to be configured to support the polarity reversal pulse. Other attributes do not need to be modified if there is no special requirement.

Copyright © Huawei Technologies Co., Ltd.

Item		Description
	Ringing current attributes	When the attributes of ring current are changed, ring volume is changed accordingly. Generally, no adjustment is required for the ringing tone volume. You need to modify the parameters of the ringing current attributes according to the local standard only when the default ringing current attributes do not comply with the local standard.

12.2.5 Principle of IPTV Service Data Plan

The IPTV service data plan mainly include the plan of VLAN and VLAN translation policy in different network scenario, and the plan of IPTV service.

IPTV services include multicast service and video on demand (VoD) service. These two services are relevant but independent in VLAN planning.

VLAN and VLAN Translation Policy.

Application Scenario	Service Type	VLAN Plan	VLAN Translation Policy
Bridging ONU + Router	Multicast service	Single-tagged VLAN	ONUs transparently transmit upstream packets with M-VLANs sent from STB. Multicast packets are replicated downstream with M-VLAN unchanged. The OLT replicates multicast packets based on PON ports with M-VLAN unchanged.
		Single-tagged VLAN	ONUs translate the upstream VLANs sent from STB to M-VLANs. The OLT replicates multicast packets based on PON ports with M-VLAN unchanged.
	VoD	Single-tagged VLAN	ONUs transparently transmit the upstream U-VLANs sent from router. The OLT implements VLAN translation: U->S.
		Double-tagged VLAN	ONUs transparently transmit the upstream U-VLANs sent from router. The OLT implements VLAN translation: U->S+C.

Copyright © Huawei Technologies Co., Ltd.

Application Scenario	Service Type	VLAN Plan	VLAN Translation Policy
Gateway ONU	Multicast service	Single-tagged VLAN	ONUs replicate packets based on user ports and M-VLANs are removed in downstream direction. The OLT replicates multicast packets based on PON ports with M-VLAN unchanged.
	VoD	Single-tagged VLAN	ONUs add C-VLAN tags to packets. Untagged VLANs are translated to C-VLANs. The OLT implements VLAN translation: C -> S.

Note:

- UserVLAN: VLAN carried by upstream packets of user-side devices, U for short.
- C-VLAN: VLAN added based on the ONU port. For details, see the description of the Double-tagged VLAN S+C.
- Double-tagged VLAN S+C: C indicates the inner VLAN (C-VLAN) and S indicates the outer VLAN (S-VLAN).
- Double-layer VLAN S+C': C' indicates the translated inner VLAN (C'-VLAN) and S indicates the outer VLAN (SVLAN).
- Single-tagged S-VLAN: Single-tagged VLAN marked or translated by the OLT. It is generally used in a single-tagged VLAN translation scenario.
- C<->S+C': Bidirectional VLAN translation: translates the inner C-VLAN and then adds one outer S-VLAN.
- C<->S+C: Bidirectional VLAN translation: maintains the inner C-VLAN and adds one outer S-VLAN.

NOTE

- IPTV service is a closed service self-operated by carriers, and single-tagged S-VLAN is recommended.
- The same S-VLAN or different S-VLANs can be used as the M-VLAN and VoD VLAN. It is recommended that you use different S-VLANs as M-VLAN and VoD VLAN so that the upper-level device easily differentiates between the BTV service and VoD service.
- S-VLANs of VoD service can identify services and physical locations based on an entire network or an OLT. It is recommended that you set different VoIP VLANs for the OLTs connected to one VoIP SR to avoid an excessively large broadcast domain of the VoIP SR and convergence switch.

12.2.6 Principle of Security Data Plan

The security plan involves system security plan, user security plan, and service security plan. Security policy ensures service security from different aspects.

Copyright © Huawei Technologies Co., Ltd.

NOTE

- The device provides complete security measures, but not all security measures need to be deployed. Only the security measures that meet the following requirements need to be deployed:
  - The security measures can be used on the live network.
  - The security measures are easy to deploy.
  - The security measures are effective.
- Different ONUs support different security features. Select the security feature recommended in this topic according to actual ONU capabilities.

System Security

Security Vulnerability	Solution	Description and Usage Suggestion
DoS attack	Enable the anti-DoS-attack function for OLT and MDU.	After the anti-DoS-attack function is enabled, control packets are monitored and those exceeding the number threshold are discarded. Use this solution for new site deployment.
IP attack	Enable the anti-IP-attack function for OLT and MDU.	After the anti-IP-attack function is enabled, a device discards the IP packets received from the user side whose destination IP address is the IP address of the device, and therefore the system is protected. Use this solution for new site deployment.

User Security

Security Vulnerability	Solution	Description and Usage Suggestion
MAC spoofing	Enable the anti-MAC-duplicate function for OLT and MDU.	After anti-MAC-duplicate is enabled, the system records the first MAC address learnt from the port and binds the MAC address to the port and VLAN. If receiving packets sent from the host that has the same MAC address with the port, the system discards the packets directly. In this case, it can prevent users from forging MAC addresses to perform malicious attacks. Use this solution for new site deployment.

Copyright © Huawei Technologies Co., Ltd.

Security Vulnerability	Solution	Description and Usage Suggestion
MAC attack	Enable the anti-MAC spoofing function for OLT and MDU.	After anti-MAC spoofing is enabled, the system can prevent users from forging IP addresses to perform malicious attacks. Use this solution for new site deployment.
IP spoofing	Enable the anti-IP spoofing function for MDU.	After anti-IP spoofing is enabled, the system can prevent users from forging IP addresses to perform malicious attacks. Use this solution for new site deployment.

Service Security

Security Vulnerability	Solution	Description and Usage Suggestion
Unauthorized broadband access of small enterprises (IPoE)	DHCP option 82 is enabled on OLT and MDU, and the BRAS implements user authentication based on the RAIO information.	In the DHCP option 82 mode, user's physical location is added to the option 82 field carried in the DHCP request packet initiated by a user. The physical location, used for user authentication on the upper-layer authentication server, can help implement the following functions: ● The DHCP relay forwards DHCP response packets to devices with specified CID and RID. ● Prevents DHCP address exhaustion. ● Achieves static allocation of DHCP addresses. ● Implements anti-IP spoofing. ● Implements anti-user ID spoofing. ● Implements anti-MAC spoofing. Use this solution for the DHCP Internet access service.

Copyright © Huawei Technologies Co., Ltd.

Security Vulnerability	Solution	Description and Usage Suggestion
Broadband access of residential users (PPPoE), user account theft/ borrowing	PPPoE+ (PITP) is enabled on OLT and MDU, and the BRAS implements user authentication based on binding of the RAIO information to the user account.	The BRAS responds to request packets of users with specified CID and RID. In this way, the following functions are implemented: ● Prevents IP address exhaustion. ● Implements anti-IP spoofing. ● Implements anti-user ID spoofing. ● Implements anti-MAC spoofing. Use this solution for the PPPoE Internet access service.

12.2.7 Principle of Reliability Data Plan

Reliability planning covers planning of equipment reliability and upstream/downstream networking protection. Reliability planning helps to achieve high reliability of FTTO SOHO and SME services.

Equipment Reliability

Protection Scheme	Description	Suggestion
Main control board 1 +1 protection	The system uses two main control boards of the same model and version. The two main control boards work in the active/standby mode by default. When the active main control board fails, the system switches to the standby main control board to prevent service interruption.	Mandatory
Power board 1+1 protection	A subrack is configured with two power boards of the same model and version, which back up each other. When one of the power board fails, the other power board can still provide power supply to the device and so the system can still work properly.	Mandatory

Copyright © Huawei Technologies Co., Ltd.

Protection Scheme	Description	Suggestion
Upstream board 1+1 protection	The system uses two upstream interface boards of the same model and version. Each GIU board provides one upstream port and two upstream ports are bound together using Link Aggregation Control Protocol (LACP). When the active upstream port fails, traffic will be transmitted upstream through the standby upstream port.	This protection scheme is recommended when the GIU board is used to transmit traffic upstream.

Upstream Networking Protection

Protection Scheme	Description	Suggestion
Link aggregation group	Multiple Ethernet ports are bound together as an aggregation group to increase the bandwidth and balance the inbound and outbound load of each member port. In addition, the ports in an aggregation group back up each other, which enhances the reliability of links.	This protection scheme is mandatory when the GIU board is used to transmit traffic upstream.
Protection group (Ethernet/STM-1)	A protection group of upstream ports contains a working port and a protection port. In normal state, the working port carries services and the protection port does not. When the link at the working port is faulty, the system automatically switches services from the working port to the protection port to ensure normal service transmission and protect the uplink.	When the main control board is used to transmit traffic upstream, this protection scheme is mandatory. This protection scheme is recommended when traffic is transmitted upstream through STM-1 ports.

NOTE

Link aggregation group and Ethernet protection group usually are not configured at the same time. You are advised to configure only one of the two protection schemes.

Copyright © Huawei Technologies Co., Ltd.

Downstream Networking Protection

Protection Scheme	Description	Suggestion
xPON Type B	Two PON ports on the same OLT back up each other. When one of the PON ports fails, the system automatically switches to the other PON port. This protection scheme provides port-level protection with low costs. It protects services against fiber failure at the working port.	It rovides port-level protection and has a low cost. The inter-board protection mode is recommended.
GPON Type C single homing	Two PON ports on the same OLT, two PON ports on an ONU, two backbone optical fibers, two optical splitters, and two tributary optical fibers are configured to provide link-level protection.	It rovides link-level protection.
GPON Type C dual homing	Two PON ports on different OLTs, two PON ports on an ONU, two backbone optical fibers, two optical splitters, and two tributary optical fibers are configured to implement this protection. The difference between this protection scheme and the GPON Type C single homing protection scheme is that the ONU needs to be dual homed to two OLTs in this protection scheme. This full-backup protection scheme provides the highest-level protection for links and has the highest costs.	It provides full backup protection, which is the highest level of protection, at the same time, it has the highest cost. This protection scheme can be configured for only the Ethernet QinQ private line service. It does not support TDM services, including Native TDM and SAToP.

NOTE

The Type B protection scheme, Type C single homing scheme, and Type C dual homing protection scheme are mutually exclusive. Therefore, only one of these protection schemes can be configured for an ONU.

12.3 SOHO Service Configuration (GPON)

This section describes Internet access, voice, and video service configurations for small office and home office (SOHO) users in GPON access mode in fiber to the office (FTTO) scenarios.

12.3.1 Service Requirements and Usage Scenario

Small office and home office (SOHO) is positioned for miniature enterprises, such as shops and markets, and home officers.

Copyright © Huawei Technologies Co., Ltd.

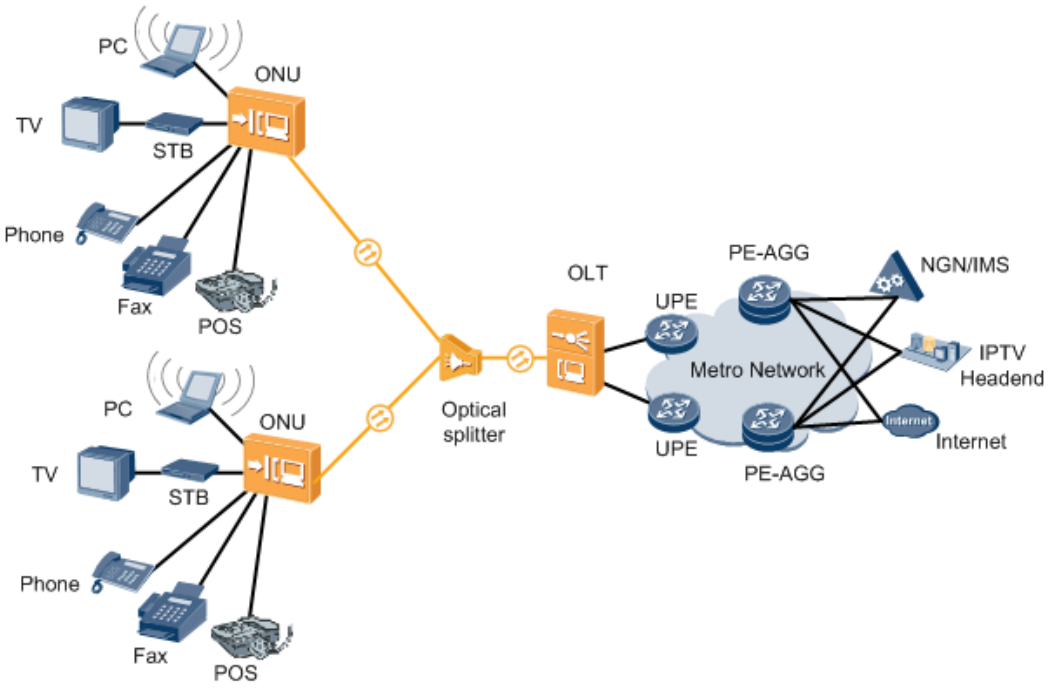
Service Requirements

In the SOHO scenario, optical network units (ONUs) work in gateway mode. Similar to home users, SOHO users require Internet, voice, and multicast services.

- The Internet can be accessed through not only cables but also wireless fidelity (Wi-Fi). A SOHO user connects to an ONU through the LAN port on the user's computer. The Dynamic Host Configuration Protocol (DHCP) address pool of the ONU assigns an IP address to the user. After PPPoE dialup is automatically performed on the ONU, the ONU connects to the OLT in GPON access mode and then connects to the upper-layer network, to provide the high-speed Internet access service for the SOHO user.
- Many voice service ports are required to connect to phone sets, fax machines, and point of sale (POS) machines.
- TVs connect to an ONU through set top boxes (STBs) to receive VoD and multicast services.
- The Internet access, voice, and IPTV services are secure.
  - The Internet access service is protected against unauthorized access, user account forgery or unauthorized borrowing, MAC or IP address spoofing, and attacks from malicious users.
  - The voice and IPTV services are protected against MAC or IP address spoofing, attacks from malicious users, and heavy traffic.
- A service fault is easy to locate, and services are easy to maintain.

Usage Scenario

Figure 12-1 SOHO networking

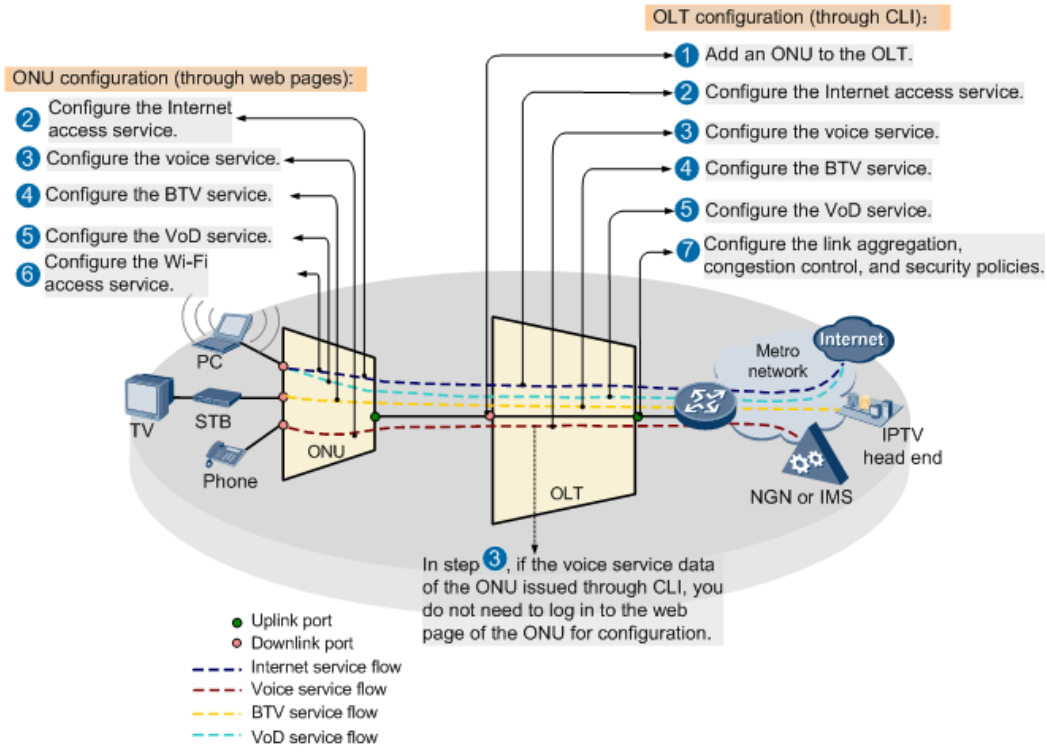


Copyright © Huawei Technologies Co., Ltd.

12.3.2 Configuration Procedure

Figure 12-2 shows the configuration procedure in the FTTO small office home office (SOHO) scenario.

Figure 12-2 Configuration procedure in the FTTO SOHO scenario



The following table lists the detailed description steps.

Item	Procedure		Remarks
OLT	**Adding an ONU to an OLT**		Services can be configured for an ONU only after the ONU is successfully added to an OLT.
OLT ONU	**Configuring the Internet Access Service**		-
OLT ONU	Configuring the Voice Service	**Configuring the H.248-based Voice Service (on a Web Page)**	**NOTE** The H.248 and SIP protocols are mutually exclusive for the VoIP service. Only one of them is configured at a time.

Copyright © Huawei Technologies Co., Ltd.

Item	Procedure		Remarks
		Configuring the H.248-based Voice Service (Through the CLI)	
		Configuring the SIP-based Voice Service (on a Web Page)	
		Configuring the SIP-based Voice Service (Through the CLI)	
OLT	**Configuring the BTV Service**		IPTV services include the VoD and multicast services that are different in configuration procedures and need to be configured separately.
OLT			
OLT	**Configuring Link Aggregation, Congestion Control, and Security Policy**		Service reliability is improved by configuring uplink aggregation and priority scheduling policy for queues in global configuration mode, and service security is improved by configuring security policy in global configuration mode.
OLT	**Verifying Services**		The OLT provides remote verification methods including ONU PPPoE and DHCP dialup emulation and call emulation for configuration and commissioning engineers to verify services remotely after service configuration, avoiding a second on-site operation.

12.3.3 Adding an ONU to an OLT

Services can be configured for an ONU only after the ONU is successfully added to an OLT.

Copyright © Huawei Technologies Co., Ltd.

Data Plan

Table 12-3 Data plan

Item	Data
DBA profile	Profile name: ftto_dba Profile type: type3 Assured bandwidth: 8 Mbit/s Maximum bandwidth: 50 Mbit/s
ONU line profile	Profile name: ftto_line T-CONT ID: 4 GEM port ID for management services: 11 GEM port ID for voice services: 12 GEM port ID for video services: 13 GEM port ID for Internet access services: 14
ONU service profile	Profile name: ftto_ser ONU port capability set: adaptive
Network topology data	PON port: 0/1/0 ONU IDs: 1 and 2

Procedure

Step 1 Configure GPON ONU profiles.

GPON ONU profiles include the DBA profile, line profile, service profile, and alarm profile.

- DBA profile: A DBA profile describes GPON traffic parameters. A T-CONT is bound to a DBA profile for dynamic bandwidth allocation, improving upstream bandwidth utilization.
- Line profile: A line profile describes the binding between the T-CONT and the DBA profile, the QoS mode of the traffic stream, and the mapping between the GEM port and the ONU-side service.
- Service profile: A service profile provides the service configuration channel for the ONU that is managed by using optical network terminal management and control interface (OMCI).
- Alarm profile: An alarm profile contains a series of alarm thresholds to measure and monitor the performance of activated ONU lines. When a statistical value reaches the threshold, the host is notified and an alarm is reported to the log host and the NMS.

1. Configure a DBA profile.

   Run the **display dba-profile** command to query existing DBA profiles in the system. If the existing DBA profiles in the system do not meet the requirements, run the **dba-profile add** command to add a DBA profile.

Copyright © Huawei Technologies Co., Ltd.

Create the same DBA profile for different types of services. Set the profile name to **ftto_dba**, profile type to **type3**, assured bandwidth to 8 Mbit/s, and maximum bandwidth to 50 Mbit/s.

```
huawei(config)#dba-profile add profile-name ftto_dba type3 assure 8192 max
51200
```

NOTE

The DBA implementation is based on an ONU. Therefore, select a DBA profile of the proper bandwidth type and configure proper bandwidth according to the service types and total user count of the ONU. Note that the sum of the fixed bandwidth and the assured bandwidth must not be greater than the total bandwidth of the PON port.

2. Configure an ONU line profile.

   Create a GPON ONU line profile, named **ftto_line**, and bind it to the DBA profile **ftto_dba**.

   ```
   huawei(config)#ont-lineprofile gpon profile-name ftto_line
   huawei(config-gpon-lineprofile-1)#tcont 4 dba-profile-name ftto_dba
   ```

   Create different GEM ports according to different service types, in which

   - GEM port 11 is used to carry management services.
   - GEM port 12 is used to carry voice services.
   - GEM port 13 is used to carry video services.
   - GEM port 14 is used to carry Internet access services.

   ```
   huawei(config-gpon-lineprofile-1)#gem add 11 eth tcont 4
   huawei(config-gpon-lineprofile-1)#gem add 12 eth tcont 4
   huawei(config-gpon-lineprofile-1)#gem add 13 eth tcont 4
   huawei(config-gpon-lineprofile-1)#gem add 14 eth tcont 4
   ```

   NOTE

   1. To change the default QoS mode, run the **qos-mode** command to set the QoS mode to **gem-car** or **flow-car**, and run the **gem add** command to set the index of the traffic profile bound to the GEM port.
   2. When the QoS mode is priority-queue (PQ), the default queue priority is 0; when the QoS mode is flow-car or gem-car, traffic profile 6 is bound to the GEM port by default (no rate limitation).

   After the configurations are complete, run the **commit** command to apply the parameters settings.

   ```
   huawei(config-gpon-lineprofile-1)#commit
   huawei(config-gpon-lineprofile-1)#quit
   ```

3. Configure an ONU service profile.

   Create a GPON ONU service profile, named **ftto_ser**. Configure the capability set of the ETH port and POTS port to **adaptive**. Then the system automatically adapts to the ONU according to the actual capability of the online ONU.

   ```
   huawei(config)#ont-srvprofile gpon profile-name ftto_ser
   huawei(config-gpon-srvprofile-1)#ont-port eth adaptive pots adaptive
   ```

   After the configurations are complete, run the **commit** command to apply the parameters setting.

   ```
   huawei(config-gpon-srvprofile-1)#commit
   huawei(config-gpon-srvprofile-1)#quit
   ```

4. (Optional) Add an alarm profile.

   - The default GPON alarm profile 1 is used. The alarm thresholds of the default alarm profile are 0, which indicates that no alarm is generated.
   - In this example, the default alarm profile is used, and therefore the configuration of the alarm profile is not required.

Copyright © Huawei Technologies Co., Ltd.

- Run the **gpon alarm-profile add** command to configure a GPON alarm profile, which is used for monitoring the performance of an activated ONU line.

Step 2 Add an ONU.

Connect two ONUs to GPON port 0/1/0. Set the ONU IDs to **1** and **2**, SNs to **32303131D659FD40** and **6877687714852901**, passwords to **0100000001** and **0100000002**, discovery mode for password authentication to **once-on**, and management mode to **OMCI**. Bind the two ONUs to ONU line profile **ftto_line** and ONU service profile **ftto_ser**.

There are two methods of adding an ONU: add an ONU offline and confirm an automatically discovered ONU.

- Add ONUs offline.

  If the password of an ONU is known, run the **ont add** command to add an ONU offline.

```
huawei(config)#interface gpon 0/1
huawei(config-if-gpon-0/1)#ont add 0 1 password-auth 0100000001 once-on no-aging
omci ont-lineprofile-name
 ftto_line ont-srvprofile-name ftto_ser
huawei(config-if-gpon-0/1)#ont add 0 2 password-auth 0100000002 once-on no-aging
omci ont-lineprofile-name
 ftto_line ont-srvprofile-name ftto_ser
```

- Confirm automatically discovered ONUs

  If the password or SN of an ONU is unknown, run the **port** ***portid*** **ont-auto-find** command in GPON mode to enable the ONU auto-discovery function of the GPON port. Then, run the **ont confirm** command to confirm the ONU.

```
huawei(config)#interface gpon 0/1
huawei(config-if-gpon-0/1)#port 0 ont-auto-find enable
huawei(config-if-gpon-0/1)#display ont autofind 0
  //After this command is executed, the information about all ONUs connected to
the GPON port through optical splitters is displayed.

huawei(config-if-gpon-0/1)#ont confirm 0 ontid 1 sn-auth 32303131D659FD40 omci
ont-lineprofile-name
 ftto_line ont-srvprofile-name ftto_ser
huawei(config-if-gpon-0/1)#ont confirm 0 ontid 2 sn-auth 6877687714852901 omci
ont-lineprofile-name
 ftto_line ont-srvprofile-name ftto_ser
```

  NOTE

  If multiple ONUs of the same type bound to the same line profile or service profile are connected to the same port, you can bulk add ONUs by bulk confirming automatically discovered ONUs to make configuration easier and more efficient. To do so, the preceding command can be modified as follows:

```
huawei(config-if-gpon-0/1)#ont confirm 0 all sn-auth omci ont-lineprofile-name
ftto_line
ont-srvprofile-name ftto_ser
```

- (Optional) Bind the alarm profile to the ONU.

  The default profile 1 is used in this example.

```
huawei(config-if-gpon-0/1)#ont alarm-profile 0 1 profile-id 1
huawei(config-if-gpon-0/1)#ont alarm-profile 0 2 profile-id 1
```

Step 3 Check ONU status.

After an ONU is added, run the **display ont info** command to query the current status of the ONU. Ensure that **Config flag** of the ONU is **active**, **Run State** is **online**, **Config state** is **normal**, and **Match state** is **match**.

```
huawei(config-if-gpon-0/1)#display ont info 0 1
  ------------------------------------------------------------------------
```


Copyright © Huawei Technologies Co., Ltd.

```
  F/S/P                : 0/1/0
  ONT-ID               : 1
  Control flag         : active    //Indicates that the ONU is
activated.
  Run state            : online    //Indicates that the ONU goes online
successfully.
  Config state         : normal    //Indicates that the configuration state of the
ONU is normal.
  Match state          : match     //Indicates that the capability profile bound to
the ONU is consistent with the actual capability of the ONU.
...//The rest of the response information is omitted.
```

When **Config state** is **failed**, **Run state** is **offline**, or **Match state** is **mismatch**:

- If **Control flag** is **deactive**, run the **ont active** command in GPON mode to activate the ONU.
- If **Run state** is **offline**, a physical line may be broken or the optical module may be damaged. Check the line and the optical module.
- If **Config state** is **failed**, the configured ONU capability exceeds the actual ONU capability. In this case, run the **display ont failed-configuration** command in the diagnose mode to check the failed configuration item and the failure cause. Then, rectify the fault accordingly.
- If the ONU does not match, that is, **Match state** is **mismatch**, the port types and number of ports undermatch the actual port types and number of ports supported by the ONU. In this case, run the **display ont capability** command to query the actual capability of the ONU, and then select one of the following modes to modify the ONU configuration:
  - Create a proper ONU profile according to the actual capability of the ONU, and then run the **ont modify** command to modify the configuration data of the ONU.
  - Modify the ONU profile according to the actual capability of the ONU and save the modification. Then, the ONU automatically recovers the configuration successfully.

----End

12.3.4 Configuring the Internet Access Service

The OLT is connected to the remote ONU through a GPON port to provide users with high-speed Internet access services.

Prerequisite

- The OLT is connected to the BRAS.
- Related configurations are performed on the BRAS according to the authentication and accounting requirements for dialup users. For details about the configuration, see the configuration guide.
- The ONU has been added to the OLT. For details, see **12.3.3 Adding an ONU to an OLT**.

Copyright © Huawei Technologies Co., Ltd.

Data Plan

Table 12-4 Data plan

Item	Data
ONU line profile	Profile name: ftto_line T-CONT ID: 4 GEM port ID for Internet access service: 14
ONU service profile	Profile name: ftto_ser ONU port capability set: adaptive

Procedure

- Configure the OLT.
  1. Configure a traffic profile.

     Run the **display traffic table ip** command to query existing traffic profiles in the system. If the traffic profiles existing in the system do not meet the requirements, you need to run the **traffic table ip** command to add a traffic profile.

     Set the profile ID to ftto_hsi, the CIR to 4 Mbit/s, and the priority to 0. In addition, configure the scheduling mode so that packets are scheduled according to their priorities.

     ```
     huawei(config)#traffic table ip name ftto_hsi cir 4096 priority 0 priority-policy local-setting
     ```

  2. Configure the mapping between a GEM port and a VLAN. Create a service VLAN and a service flow.

     Table 12-5 Scenario plan

Scenario	VLAN Plan	VLAN Translation Policy
gateway ONU	Double-tagged VLAN - S-VLAN ID: 100 - S-VLAN type: smart - S-VLAN attribute: stacking - C-VLAN ID: 1001 - C'-VLAN ID: 1010-1011	ONU: Configure a VLAN for all ONUs and add the same C-VLAN tag to packets. All ONUs are in the same C-VLAN. OLT: The OLT switches between the C-VLAN tag and the S-VLAN +C'-VLAN tag. All ONUs are in different C-VLANs.

Copyright © Huawei Technologies Co., Ltd.

Configure the mapping between a GEM port and a VLAN. The service flow of user VLAN 1001 is mapped to GEM port 14 in the ONU line profile.

```
huawei(config)#ont-lineprofile gpon profile-name ftto_line
huawei(config-gpon-lineprofile-1)#gem mapping 14 0 vlan 1001
huawei(config-gpon-lineprofile-1)#commit
huawei(config-gpon-lineprofile-1)#quit
```

Create a service VLAN and add an upstream port to it. Add upstream port 0/19/0 to VLAN 100.

```
huawei(config)#vlan 100 smart
huawei(config)#vlan attrib 100 stacking
huawei(config)#port vlan 100 0/19 0
```

Create service flows. Set the service VLAN to 100, GEM port ID to 14, and user VLAN to 1001, and use traffic profile ftto_hsi.

```
huawei(config)#service-port vlan 100 gpon 0/1/0 ont 1 gemport 14 multi-
service
user-vlan 1001 tag-transform translate-and-add inner-vlan 1010 inbound
traffic-table name
ftto_hsi outbound traffic-table name ftto_hsi
huawei(config)#service-port vlan 100 gpon 0/1/0 ont 2 gemport 14 multi-
service
user-vlan 1001 tag-transform translate-and-add inner-vlan 1011 inbound
traffic-table name
ftto_hsi outbound traffic-table name ftto_hsi
```

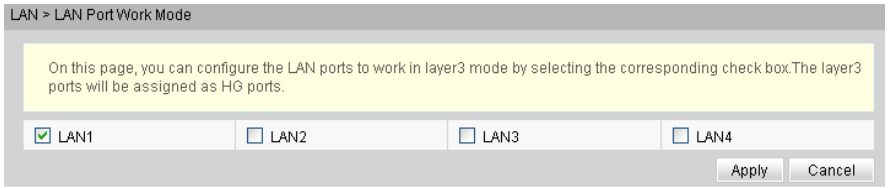
3. Save the data.

```
huawei(config)#save
```

- Configure an optical network terminal (ONU) on the Web page.

  Layer 3 route mode is used for connecting an ONU to the upper-layer device. IP addresses of users' PCs are allocated by the DHCP IP address pool on the ONU. PPPoE auto dialup is performed on the ONU. Parameters of the WAN port must be configured on the ONU.

  1. Log in to the Web configuration window.
     a. Configure the IP address of the PC network adapter to be in the same network segment as the IP address of the local maintenance Ethernet port on the ONU (default: **192.168.100.1**).
     b. Open the Web browser, and enter the IP address of the local maintenance Ethernet port of the ONU.
     c. On the login window, enter the user name (default: **telecomadmin**) and password (default: **admintelecom**) of the administrator. After the password authentication is passed, the Web configuration interface is displayed.
  2. Configure the working mode of a LAN port.
     a. In the navigation tree, choose **LAN** > **LAN Port Work Mode**. Select the check box of LAN 1 and set LAN1 to work in the Layer 3 mode.

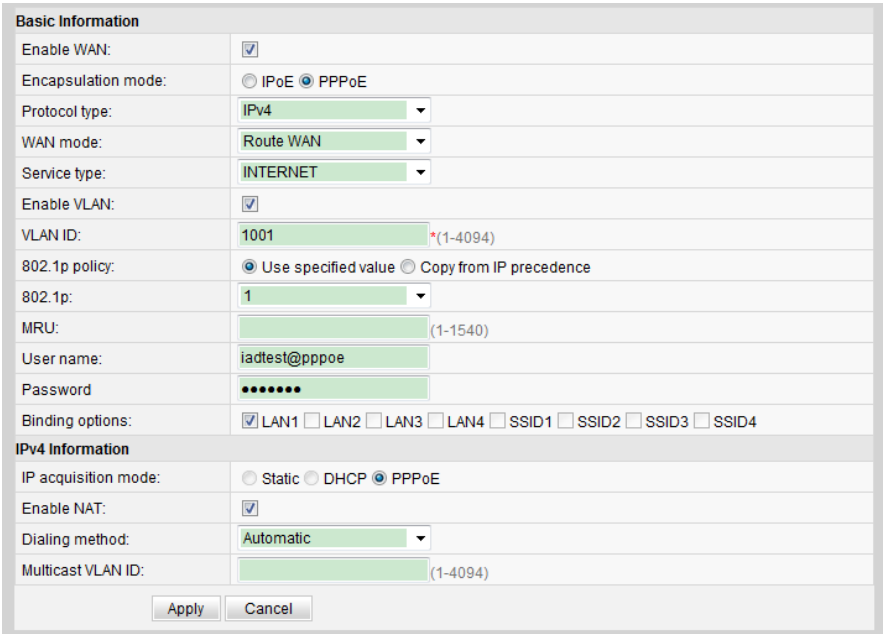
     b. Click **Apply** to apply the configuration.
  3. Configure parameters of a WAN port.

Copyright © Huawei Technologies Co., Ltd.

a. In the navigation tree, choose **WAN** > **WAN Configuration**.

b. In the right pane, click **New**. In the dialog box that is displayed, configure parameters of a WAN port as follows:

- WAN Connection: Enable
- Encapsulation Mode: PPPoE
- WAN mode: Route WAN
- Service type: INTERNET (For configuring the Internet access service, **INTERNET** or a combination containing **INTERNET** needs to be selected.)
- VLAN ID: 1001 (The VLAN ID of the ONU must be the same as the user-side VLAN ID configured on the OLT.)
- 802.1p: 1
- User Name: iadtest@pppoe, Password: iadtest (The user name and password must be the same as the user name and password configured on the BRAS.)
- Binding options: LAN1
- IP acquisition Mode: PPPoE
- NAT: Enable (NAT must be enabled to configure the Internet access service.)

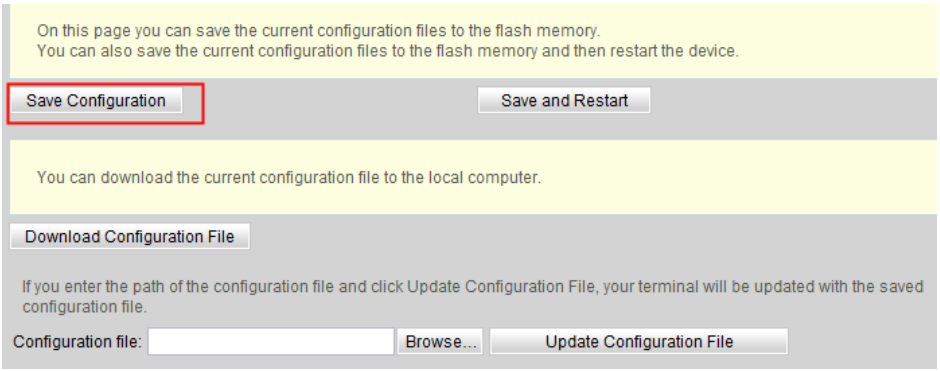


c. Click **Apply** to apply the configuration.

4. Save the configuration.

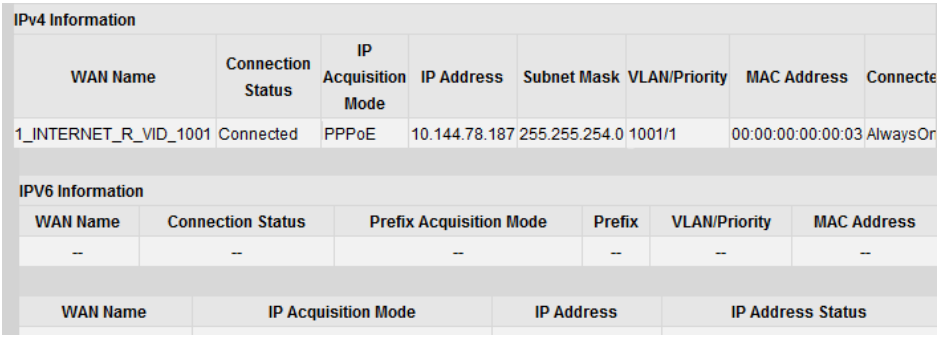
   In the navigation tree, choose **System Tools** > **Configuration File**. In the right pane, click **Save Configuration** to save the configuration.

Copyright © Huawei Technologies Co., Ltd.



5. Check the ONU connection status.

   In the navigation tree, choose **Status** > **WAN Information**. In the right pane, **Status** is **Connected** and the obtained IP address is displayed at **IP Address**.



IPv4 Information

WAN Name	Connection Status	IP Acquisition Mode	IP Address	Subnet Mask	VLAN/Priority	MAC Address	Connecte
1_INTERNET_R_VID_1001	Connected	PPPoE	10.144.78.187	255.255.254.0	1001/1	00:00:00:00:00:03	AlwaysOr

IPV6 Information

WAN Name	Connection Status	Prefix Acquisition Mode	Prefix	VLAN/Priority	MAC Address
--	--	--	--	--	--

WAN Name	IP Acquisition Mode	IP Address	IP Address Status

----End

12.3.5 Configuring the H.248-based Voice Service (on a Web Page)

The OLT is connected to the remote ONU through a GPON port to provide users with the IP-based high-quality and low-cost VoIP service.

Prerequisite

- The interface data and POTS port data corresponding to the MG interface have been configured on the MGC.
- The OLT has been connected to the MGC. The OLT can ping the IP address of the MGC server successfully.
- The ONU has been added to the OLT. For details, see **12.3.3 Adding an ONU to an OLT**.
- Different voice services require different ONU software versions. Before the configuration, ensure that the ONU software version supports H.248. For details, see relevant ONU manuals.

Copyright © Huawei Technologies Co., Ltd.

Context

Table 12-6 Data plan

Item	Data
ONU line profile	Profile name: ftto_line T-CONT ID: 4 GEM port ID: 12
ONU service profile	Profile name: ftto_ser ONU port capability set: adaptive
Networking data	IP address of the MGC server: 200.200.200.200/24 Port ID of the MGC server: 2944

Procedure

- Configure the OLT.
  1. Configure a traffic profile.

     Set the profile name to **ftto_voip** and do not limit the upstream and downstream rates. Set the priority to **5** and packets are scheduled according to the priority carried.

     Run the **display traffic table ip** command to query existing traffic profiles in the system. If the existing traffic profiles in the system do not meet the requirements, run the **traffic table ip** command to add a traffic profile.

     ```
     huawei(config)#traffic table ip name ftto_voip cir off priority 5 priority-policy
      local-setting
     ```

  2. Configure the mapping between a GEM port and a VLAN. Create a service VLAN and a service flow.

     Table 12-7 Scenario plan

Scenario	VLAN Plan	VLAN Translation Policy
Scenario 1	Single VLAN tag ● S-VLAN ID: 300 ● S-VLAN type: smart ● S-VLAN attribute: common ● C-VLAN ID: 300	ONU: Configure a VLAN for all ONUs and add the same C-VLAN tag to packets. All ONUs are in the same C-VLAN. OLT: The OLT transparently transmits VLAN tags (the C-VLAN is the same as the planned S-VLAN).

Copyright © Huawei Technologies Co., Ltd.

Scenario	VLAN Plan	VLAN Translation Policy
Scenario 2	Single VLAN tag ● S-VLAN ID: 300 ● S-VLAN type: smart ● S-VLAN attribute: common ● C-VLAN ID: 3001	ONU: Configure a VLAN for all ONUs and add the same C-VLAN tag to packets. All ONUs are in the same C-VLAN. OLT: The OLT switches between C-VLAN tags and S-VLAN tags (C-VLAN is different from the planned S-VLAN).

Scenario 1:

Configure the mapping between a GEM port and a VLAN. The service flow of user VLAN 300 is mapped to GEM port 12 in the ONU line profile.

```
huawei(config)#ont-lineprofile gpon profile-name ftto_line
huawei(config-gpon-lineprofile-1)#gem mapping 12 2 vlan 300
huawei(config-gpon-lineprofile-1)#commit
huawei(config-gpon-lineprofile-1)#quit
```

Create a service VLAN and add an upstream port to it. Add upstream port 0/19/0 to VLAN 300.

```
huawei(config)#vlan 300 smart
huawei(config)#port vlan 300 0/19 0
```

Create service flows. Set the service VLAN to 300, GEM port ID to 12, and user VLAN to 300, and use traffic profile **ftto_voip**.

```
huawei(config)#service-port vlan 300 gpon 0/1/0 ont 1 gemport 12 multi-
service
 user-vlan 300 inbound traffic-table name ftto_voip outbound traffic-table
name
ftto_voip
huawei(config)#service-port vlan 300 gpon 0/1/0 ont 2 gemport 12 multi-
service
 user-vlan 300 inbound traffic-table name ftto_voip outbound traffic-table
name
ftto_voip
```

Scenario 2:

Configure the mapping between a GEM port and a VLAN. The service flow of user VLAN 3001 is mapped to GEM port 12 in the ONU line profile.

```
huawei(config)#ont-lineprofile gpon profile-name ftto_line
huawei(config-gpon-lineprofile-1)#gem mapping 12 2 vlan 3001
huawei(config-gpon-lineprofile-1)#commit
huawei(config-gpon-lineprofile-1)#quit
```

Create a service VLAN and add an upstream port to it. Add upstream port 0/19/0 to VLAN 300.

```
huawei(config)#vlan 300 smart
huawei(config)#vlan attrib 300 stacking
huawei(config)#port vlan 300 0/19 0
```


Copyright © Huawei Technologies Co., Ltd.

Create service flows. Set the service VLAN to 300, GEM port ID to 12, and user VLAN to 3001. Use traffic profile **ftto_voip**.

```
huawei(config)#service-port vlan 300 gpon 0/1/0 ont 1 gemport 12 multi-
service
user-vlan 3001 tag-transform translate inbound traffic-table name
ftto_voip outboun
d traffic-table name ftto_voip
huawei(config)#service-port vlan 300 gpon 0/1/0 ont 2 gemport 12 multi-
service
user-vlan 3001 tag-transform translate inbound traffic-table name
ftto_voip outboun
d traffic-table name ftto_voip
```

3. Enable the ARP proxy function.

   Voice media streams for different users of the same S-VLAN fail to interchange because the service ports of the smart VLAN are isolated from each other. Therefore, the ARP proxy function needs to be enabled on the OLT.

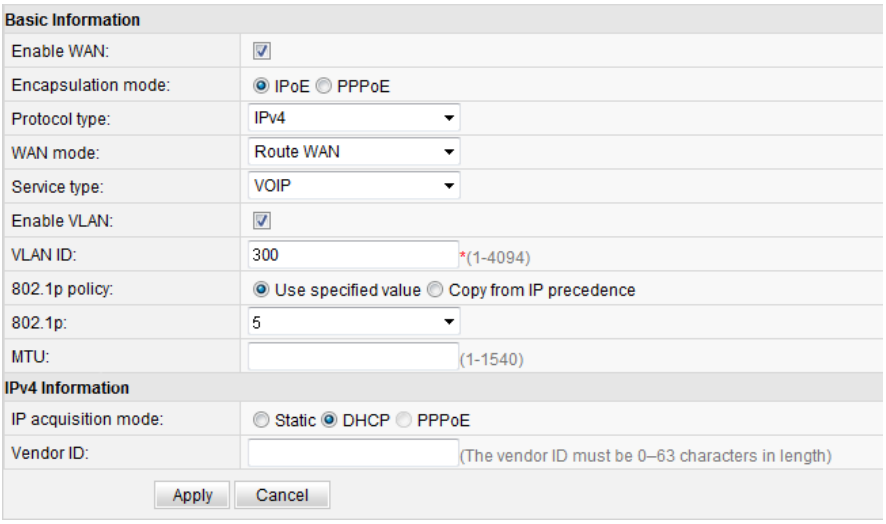
   ```
   huawei(config)#arp proxy enable
   huawei(config)#interface vlanif 300
   huawei(config-if-vlanif300)#arp proxy enable
   huawei(config-if-vlanif300)#quit
   ```

4. Save the data.

   ```
   huawei(config)#save
   ```

- Configure the ONU on the Web page.
  1. Log in to the Web configuration window.
     a. Configure the IP address of the PC network adapter to be in the same network segment as the IP address of the local maintenance Ethernet port on the ONU (default: **192.168.100.1**).
     b. Open the Web browser, and enter the IP address of the local maintenance Ethernet port of the ONU.
     c. On the login window, enter the user name (default: **telecomadmin**) and password (default: **admintelecom**) of the administrator. After the password authentication is passed, the Web configuration interface is displayed.
  2. Configure parameters of a voice WAN port.
     a. In the navigation tree, choose **WAN** > **WAN Configuration**.
     b. In the right pane, click **New**. In the dialog box that is displayed, configure parameters of a WAN port as follows:
        - WAN Connection: Enable
        - Service List: VoIP (For configuring the VoIP service, VoIP or a combination containing VoIP needs to be selected.)
        - Mode: Route
        - VLAN ID: 300 (The VLAN ID of the ONU must be the same as the user-side VLAN ID configured on the OLT.)
        - 802.1p: 5
        - IP Acquisition Mode: DHCP

Copyright © Huawei Technologies Co., Ltd.



c. Click **Apply** to apply the configuration.

3. Configure the parameters of the H.248-based voice interface.

   a. In the navigation tree, choose **Voice** > **VoIP Basic Configuration**.

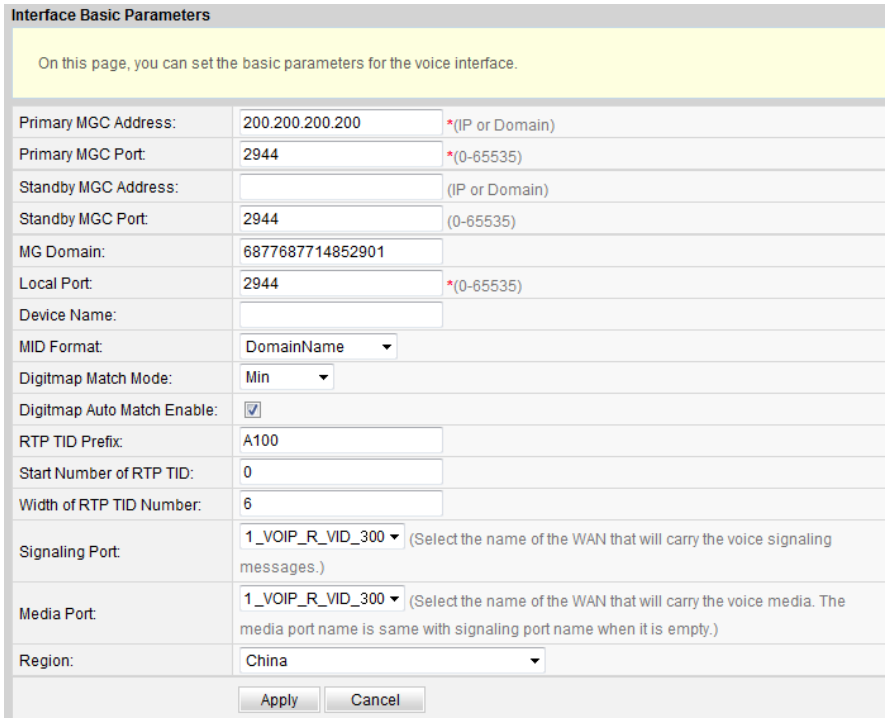
   b. In the right pane, configure the parameters of the H.248-based voice interface as follows (other parameters use the default settings):

      - Set **MGC Address** below **Primary Server** to **200.200.200.200**.
      - MID Format: DomainName
      - MG Domain: 6877687714852901
      - Signaling Port: 1_VOIP_R_VID_300
      - Region: China

      NOTE

      - The parameters of the H.248-based voice interface must be consistent with the corresponding configuration on the media gateway controller (MGC).
      - If dual-homing is configured, **MGC Address** below **Secondary Server** must be configured.
      - **MID Format** can be set to **Domain Name**, **IP**, or **Device**. If **MID Format** is set to **Domain Name** or **Device**, the setting must be consistent with the corresponding configuration on the MGC.
      - **Domain Name** is ONU's domain name registered with the MGC. It is globally unique. **Domain Name** in this example is ONU's SN.
      - If **Media Port** is empty, the parameter value is the same as **Signaling Port**. The media streams are not isolated from signaling streams. If the upper-layer network requires isolation of media streams from signaling streams, create different traffic streams for the media streams and signaling streams on the OLT, create different WAN ports on the ONU, and bind the created WAN ports to **Media Port** and **Signaling Port**.
      - **Profile Index** can be set to **Default**, **BT**, **FT**, **KPN**, **PCCW**, **ZTE**, or **BELL**. Choose the value based on the MGC type. **Profile Index** is set to **Default** (indicating interconnection with Huawei MGC) in this example. If the settings do not meet requirements, configure **UserDefine**. For details about how to configure this parameter, contact Huawei technical support engineers.
      - When the ONU is interconnected with a third-party softswitch, check **RTP TID Prefix**, **Start Number of RTP TID**, and **Width of RTP TID Number**.

Copyright © Huawei Technologies Co., Ltd.



c. Click **Apply** to apply the configuration.

4. Configure parameters of the H.248-based voice users.

a. In the navigation tree, choose **Voice** > **VoIP Basic Configuration**.

b. In the right pane, configure the parameters of voice user 1 as follows:

- Line Name: A0
- Associated POTS: 1 (binding port TEL1 on the ONU)
- Select **Enable Line Name** to enable the voice user configuration.

c. Click **Apply** to apply the configuration.

d. In the right pane, click **New** to add voice user 2, and configure the parameters of voice user 2 as follows:

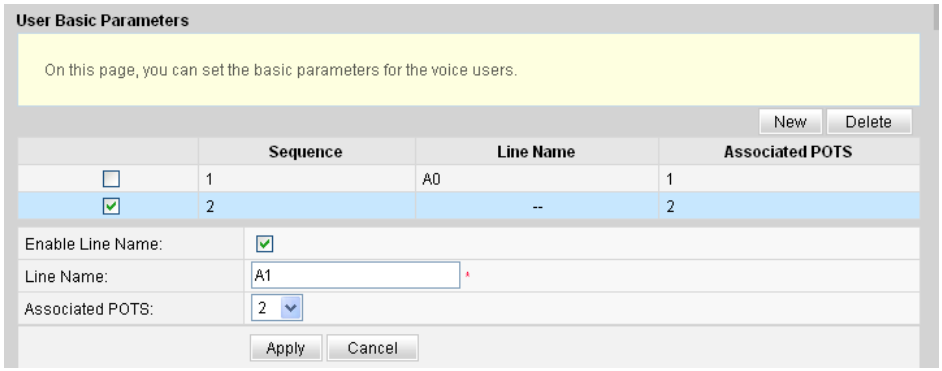
- Line Name: A1
- Associated POTS: 2 (binding port TEL2 on the ONU)
- Select **Enable Line Name** to enable the voice user configuration.

e. Click **Apply** to apply the configuration.

NOTE

- The terminal IDs **A0** and **A1** must be consistent with the corresponding configuration on the MGC.
- If **Associated POTS** is **1**, port TEL1 on the ONU is bound. If **Associated POTS** is **2**, port TEL2 on the ONU is bound.

Copyright © Huawei Technologies Co., Ltd.



5. (Optional) Configure a route.

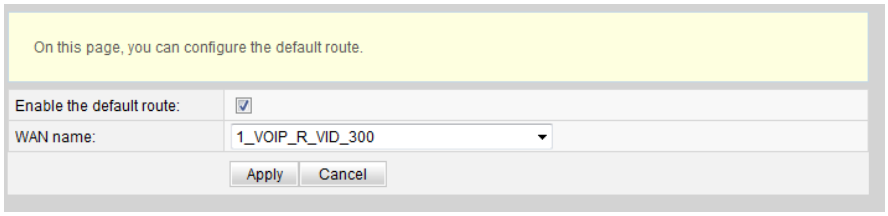
   Perform this operation if the IP address of the ONU and the IP address of the voice server are in different network segments.

   a. Choose **Route** > **Default Route Configuration** from the main menu.

   b. Select **Enable the default route** and set **WAN name** to **1_VOIP_R_VID_300**.

   Figure 12-3 shows the settings.

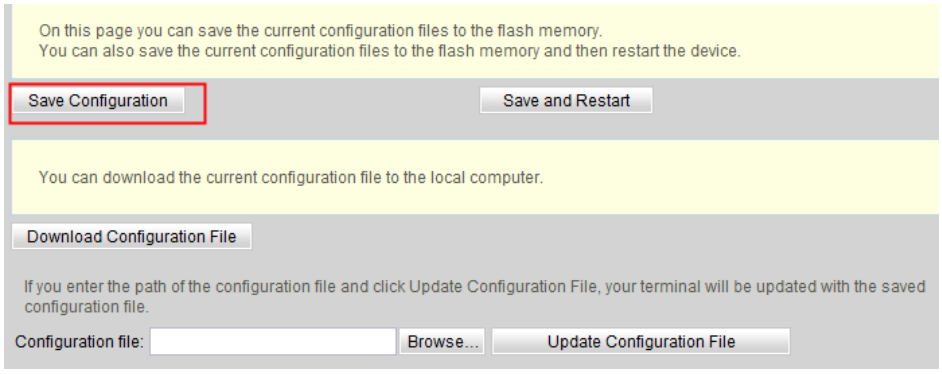
   Figure 12-3 Configuring a route



   c. Click **Apply** to apply the configuration.

6. Save the configuration.

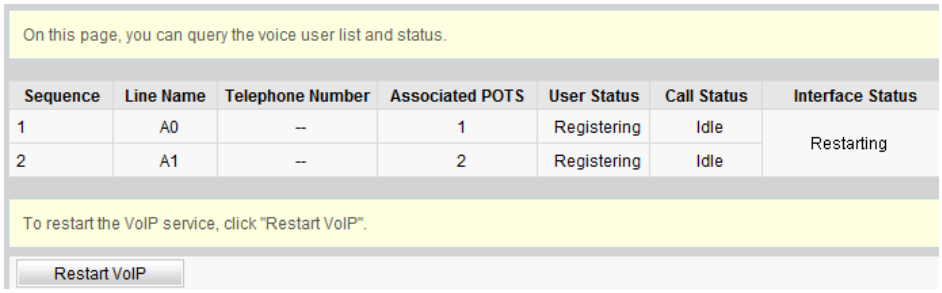
   In the navigation tree, choose **System Tools** > **Configuration File**. In the right pane, click **Save Configuration** to save the configuration.



7. Restart the voice process.

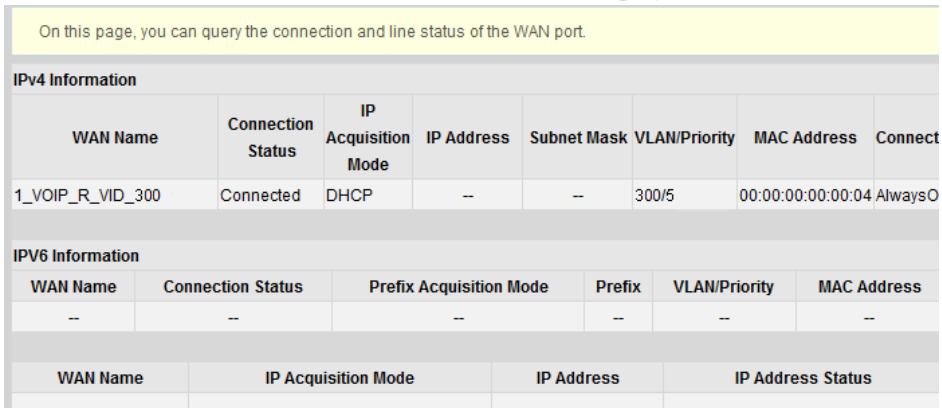
   In the navigation tree, choose **Status** > **VoIP Information**. In the right pane, click **Restart VoIP**.

Copyright © Huawei Technologies Co., Ltd.



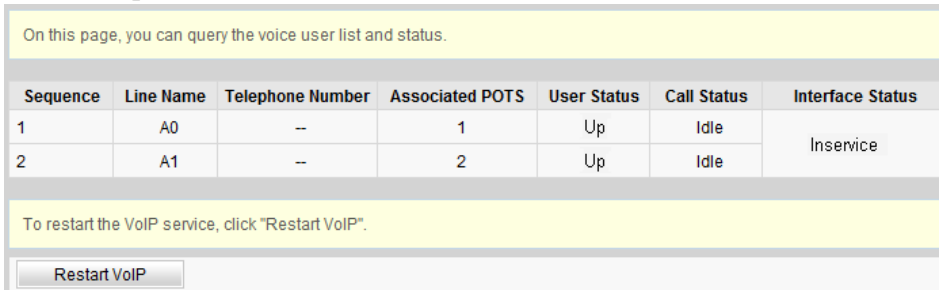
8. Check the ONU connection status.

   In the navigation tree, choose **Status** > **WAN Information**. In the right pane, **Status** is **Connected** and the obtained IP address is displayed at **IP Address**.



9. Check the registration status of a voice user.

   In the navigation tree, choose **Status** > **VoIP Information**. In the right pane, **User Status** is **Up**.



----End

12.3.6 Configuring the H.248-based Voice Service (Through the CLI)

The OLT manages ONUs and applies VoIP configurations to the ONU using the OMCI protocol. This topic describes how to configure the H.248-based voice service.

Prerequisite

- The interface data and POTS port data corresponding to the MG interface have been configured on the MGC.
- The OLT has been connected to the MGC. The OLT can ping the IP address of the MGC server successfully.

Copyright © Huawei Technologies Co., Ltd.

- The ONU has been added to the OLT. For details, see **12.3.3 Adding an ONU to an OLT**.
- Different voice services require different ONU software versions. Before the configuration, ensure that the ONU software version supports H.248. For details, see relevant ONU manuals.

Context

Table 12-8 Data plan

Item	Data
ONU line profile	Profile name: ftto_line T-CONT ID: 4 GEM port ID: 12
ONU service profile	Profile name: ftto_ser ONU port capability set: adaptive
Networking data	IP address of the MGC server: 200.200.200.200/24 Port ID of the MGC server: 2944

Procedure

Step 1 Configure a traffic profile.

Set the profile name to **ftto_voip** and do not limit the upstream and downstream rates. Set the priority to **5** and packets are scheduled according to the priority carried.

Run the **display traffic table ip** command to query existing traffic profiles in the system. If the existing traffic profiles in the system do not meet the requirements, run the **traffic table ip** command to add a traffic profile.

Step 2 Configure the mapping between a GEM port and a VLAN. Create a service VLAN and a service flow.

Table 12-9 Scenario plan

Scenario	VLAN Plan	VLAN Translation Policy
Scenario 1	Single VLAN tag ● S-VLAN ID: 300 ● S-VLAN type: smart ● S-VLAN attribute: common ● C-VLAN ID: 300	ONU: Configure a VLAN for all ONUs and add the same C-VLAN tag to packets. All ONUs are in the same C-VLAN. OLT: The OLT transparently transmits VLAN tags (the C-VLAN is the same as the planned S-VLAN).

Copyright © Huawei Technologies Co., Ltd.

Scenario	VLAN Plan	VLAN Translation Policy
Scenario 2	Single VLAN tag ● S-VLAN ID: 300 ● S-VLAN type: smart ● S-VLAN attribute: common ● C-VLAN ID: 3001	ONU: Configure a VLAN for all ONUs and add the same C-VLAN tag to packets. All ONUs are in the same C-VLAN. OLT: The OLT switches between C-VLAN tags and S-VLAN tags (C-VLAN is different from the planned S-VLAN).

Scenario 1:

Configure the mapping between a GEM port and a VLAN. The service flow of user VLAN 300 is mapped to GEM port 12 in the ONU line profile.

```
huawei(config)#ont-lineprofile gpon profile-name ftto_line
huawei(config-gpon-lineprofile-1)#gem mapping 12 2 vlan 300
huawei(config-gpon-lineprofile-1)#commit
huawei(config-gpon-lineprofile-1)#quit
```

Create a service VLAN and add an upstream port to it. Add upstream port 0/19/0 to VLAN 300.

```
huawei(config)#vlan 300 smart
huawei(config)#port vlan 300 0/19 0
```

Create service flows. Set the service VLAN to 300, GEM port ID to 12, and user VLAN to 300, and use traffic profile **ftto_voip**.

```
huawei(config)#service-port vlan 300 gpon 0/1/0 ont 1 gemport 12 multi-service
 user-vlan 300 inbound traffic-table name ftto_voip outbound traffic-table name
ftto_voip
huawei(config)#service-port vlan 300 gpon 0/1/0 ont 2 gemport 12 multi-service
 user-vlan 300 inbound traffic-table name ftto_voip outbound traffic-table name
ftto_voip
```

Scenario 2:

Configure the mapping between a GEM port and a VLAN. The service flow of user VLAN 3001 is mapped to GEM port 12 in the ONU line profile.

```
huawei(config)#ont-lineprofile gpon profile-name ftto_line
huawei(config-gpon-lineprofile-1)#gem mapping 12 2 vlan 3001
huawei(config-gpon-lineprofile-1)#commit
huawei(config-gpon-lineprofile-1)#quit
```

Create a service VLAN and add an upstream port to it. Add upstream port 0/19/0 to VLAN 300.

```
huawei(config)#vlan 300 smart
huawei(config)#vlan attrib 300 stacking
huawei(config)#port vlan 300 0/19 0
```

Create service flows. Set the service VLAN to 300, GEM port ID to 12, and user VLAN to 3001. Use traffic profile **ftto_voip**.

```
huawei(config)#service-port vlan 300 gpon 0/1/0 ont 1 gemport 12 multi-service
user-vlan 3001 tag-transform translate inbound traffic-table name ftto_voip
outboun
d traffic-table name ftto_voip
```


Copyright © Huawei Technologies Co., Ltd.

```
huawei(config)#service-port vlan 300 gpon 0/1/0 ont 2 gemport 12 multi-service
user-vlan 3001 tag-transform translate inbound traffic-table name ftto_voip
outboun
d traffic-table name ftto_voip
```

Step 3 Configure ONU voice service profiles.

ONU voice service profiles include the interface common profile, MGC interface profile, and POTS port profile.

- Interface common profile: saves common attributes of an ONU voice interface, including the fax mode, fax/modem negotiation mode, and priority of the coding and decoding mode.
- MGC interface profile: saves the IP address or domain name of the MGC, protocol port ID of the MGC transport layer to which the MG interface belongs, and DSCP priority of media packets.
- POTS port profile: saves physical attributes of a POTS port on an ONU, including the impedance, transmitting gain, receiving gain, and signaling type of the POTS port.

1. Configure an interface common profile.

   Run the **display ont-mg-attribute-profile** command to query the existing interface common profile in the system. If the existing interface common profile in the system does not meet the requirements, run the **ont-mg-attribute-profile add** command to add an interface common profile.

   In this example, the default interface common profile, namely interface common profile 1 is used.

2. Configure an MGC interface profile.

   Run the **display ont-mgc-profile** command to query the existing MGC interface profile in the system. If the existing MGC interface profile in the system does not meet the requirements, run the **ont-mgc-profile add** command to add an MGC interface profile.

   Create MGC interface profile 2, set the IP address of the MGC to 200.200.200.200, and use default values for other parameters.

   ```
   huawei(config)#ont-mgc-profile add profile-id 2 primary-mgc 200.200.200.200
   ```

3. Configure a POTS port profile.

   Run the **display ont-pots-profile** command to query the existing POTS port profile in the system. If the existing POTS port profile in the system does not meet the requirements, run the **ont-pots-profile add** command to add a POTS port profile.

   In this example, the default POTS port profile, namely POTS port profile 1 is used.

Step 4 Configure the IP addresses of ONU SIP users.

For ONU 1 and ONU 2, configure the IP address obtaining mode to the static mode, set the IP addresses to 10.10.10.10/24 and 10.10.10.20/24, set the management VLAN to VLAN 20, and use default values for other parameters.

```
huawei(config)#interface gpon 0/1
huawei(config-if-gpon-0/1)#ont ipconfig 0 1 dhcp vlan 20
huawei(config-if-gpon-0/1)#ont ipconfig 0 2 dhcp vlan 20
```

Step 5 Configure H.248 POTS users.

1. Add an H.248 interface and apply an MGC interface profile to the interface.

   For ONU 1 and ONU 2, set the MG ID to 1, apply MGC interface profile 2 to ONU 1 and ONU 2, and use default values for other parameters.

   If parameters of an MGC interface profile are changed, the MGC interface profile must be reapplied to the ONU so that the changed parameters can take effect.

Copyright © Huawei Technologies Co., Ltd.

```
huawei(config-if-gpon-0/1)#if-h248 add 0 1 1 mgc-profile profile-id 2
huawei(config-if-gpon-0/1)#if-h248 add 0 2 1 mgc-profile profile-id 2
```

2. Add POTS users.

   For ONU 1 and ONU 2, create a POTS user, set the MG ID to 1 (identical to the MG ID of the H.248 interface), and set the physical terminal port ID to A0 and A1.

```
huawei(config-if-gpon-0/1)#mgpstnuser add 0 1 1 mgid 1 terminalid A0
huawei(config-if-gpon-0/1)#mgpstnuser add 0 2 1 mgid 1 terminalid A1
```

   Run the **display mgpstnuser attribute** command to check whether the configuration of the POTS user is properly set.

```
huawei(config-if-gpon-0/1)#display mgpstnuser attribute 0 1 1

---------------------------------------------------------------------------
  F/S/P                       : 0/1/0
  ONT ID                      : 1
  Port ID                     : 1

  MG ID                       : 1
  Terminal ID                 : A0
...//The rest of the response information is omitted.

huawei(config-if-gpon-0/1)#display mgpstnuser attribute 0 2 1

---------------------------------------------------------------------------
  F/S/P                       : 0/1/0
  ONT ID                      : 2
  Port ID                     : 1

  MG ID                       : 1
  Terminal ID                 : A1
...//The rest of the response information is omitted.
```

Step 6 Apply ONU voice service profiles

After ONU voice service profiles are applied, if parameters in those profiles are changed, those profiles must be reapplied so that the changed parameters can take effect.

1. Apply an interface common profile.

   Run the **if-h248 attribute** command to apply an interface common profile to an H.248 interface or configure the interface customized parameters, or run the **ont-if-h248 bat-apply** command to bulk apply the interface common profiles to H.248 interfaces. If you use these two commands to apply the interface common profiles or configure the interface customized parameters repeatedly, the last configurations take effect.

   In this example, the default interface common profile, namely interface common profile 1 is used.

2. Apply a POTS port profile.

   Run the **pstnport electric** command to apply a POTS port profile to an H.248 interface or configure the interface customized parameters, or run the **ont-pstnport electric bat-apply** command to bulk apply the POTS port profiles to H.248 interfaces. If you use these two commands to apply the POTS port profiles or configure the interface customized parameters repeatedly, the last configurations take effect.

   In this example, the default POTS port profile, namely POTS port profile 1 is used.

Step 7 (Optional) Configure the H.248 user codec.

Run the **mgpstnuser codec** command to configure the H.248 user codec. The H.248 user codec will not be configured independently in this example.

Copyright © Huawei Technologies Co., Ltd.

Step 8 Save the data.

```
huawei(config)#save
```

----End

12.3.7 Configuring the SIP-based Voice Service (on a Web Page)

The OLT is connected to the remote ONU through a GPON port to provide users with the IP-based high-quality and low-cost VoIP service.

Prerequisite

- The SIP interface data and POTS port data corresponding to the MG interface have been configured on the SIP server.
- The connection between the OLT and the SIP server is set up. The OLT can ping the IP address of the SIP server successfully.
- The ONU has been added to the OLT. For details, see **9.7.1.3 Adding an ONT to an OLT**.
- Different voice services require different ONU software versions. Before the configuration, ensure that the current ONU software version supports SIP. For details, see relevant ONU manuals.

Data Plan

Table 12-10 Data plan

Item	Data
ONU line profile	Profile name: ftto_line T-CONT ID: 4 GEM port ID: 12
ONU service profile	Profile name: ftto_ser ONU port capability set: adaptive
Voice parameter	IP address of the SIP server: 200.200.200.200/24 Port ID of the SIP server: 5060 Home domain name: huawei.com User phone number 1: 77730010 User phone number 2: 77730020

Procedure

- Configure the OLT.
  1. Configure a traffic profile.

     Set the profile name to **ftto_voip** and do not limit the upstream and downstream rates. Set the priority to **5** and packets are scheduled according to the priority carried.

Copyright © Huawei Technologies Co., Ltd.

Run the **display traffic table ip** command to query existing traffic profiles in the system. If the existing traffic profiles in the system do not meet the requirements, run the **traffic table ip** command to add a traffic profile.

```
huawei(config)#traffic table ip name ftto_voip cir off priority 5 priority-
policy
 local-setting
```

2. Configure the mapping between a GEM port and a VLAN. Create a service VLAN and a service flow.

Table 12-11 Scenario plan

Scenario	VLAN Plan	VLAN Translation Policy
Scenario 1	Single VLAN tag ● S-VLAN ID: 300 ● S-VLAN type: smart ● S-VLAN attribute: common ● C-VLAN ID: 300	ONU: Configure a VLAN for all ONUs and add the same C-VLAN tag to packets. All ONUs are in the same C-VLAN. OLT: The OLT transparently transmits VLAN tags (the C-VLAN is the same as the planned S-VLAN).
Scenario 2	Single VLAN tag ● S-VLAN ID: 300 ● S-VLAN type: smart ● S-VLAN attribute: common ● C-VLAN ID: 3001	ONU: Configure a VLAN for all ONUs and add the same C-VLAN tag to packets. All ONUs are in the same C-VLAN. OLT: The OLT switches between C-VLAN tags and S-VLAN tags (C-VLAN is different from the planned S-VLAN).

Scenario 1:

Configure the mapping between a GEM port and a VLAN. The service flow of user VLAN 300 is mapped to GEM port 12 in the ONU line profile.

```
huawei(config)#ont-lineprofile gpon profile-name ftto_line
huawei(config-gpon-lineprofile-1)#gem mapping 12 2 vlan 300
huawei(config-gpon-lineprofile-1)#commit
huawei(config-gpon-lineprofile-1)#quit
```

Create a service VLAN and add an upstream port to it. Add upstream port 0/19/0 to VLAN 300.

```
huawei(config)#vlan 300 smart
huawei(config)#port vlan 300 0/19 0
```

Create service flows. Set the service VLAN to 300, GEM port ID to 12, and user VLAN to 300, and use traffic profile **ftto_voip**.

Copyright © Huawei Technologies Co., Ltd.

```
huawei(config)#service-port vlan 300 gpon 0/1/0 ont 1 gemport 12 multi-
service
 user-vlan 300 inbound traffic-table name ftto_voip outbound traffic-table
name
ftto_voip
huawei(config)#service-port vlan 300 gpon 0/1/0 ont 2 gemport 12 multi-
service
 user-vlan 300 inbound traffic-table name ftto_voip outbound traffic-table
name
ftto_voip
```

Scenario 2:

Configure the mapping between a GEM port and a VLAN. The service flow of user VLAN 3001 is mapped to GEM port 12 in the ONU line profile.

```
huawei(config)#ont-lineprofile gpon profile-name ftto_line
huawei(config-gpon-lineprofile-1)#gem mapping 12 2 vlan 3001
huawei(config-gpon-lineprofile-1)#commit
huawei(config-gpon-lineprofile-1)#quit
```

Create a service VLAN and add an upstream port to it. Add upstream port 0/19/0 to VLAN 300.

```
huawei(config)#vlan 300 smart
huawei(config)#vlan attrib 300 stacking
huawei(config)#port vlan 300 0/19 0
```

Create service flows. Set the service VLAN to 300, GEM port ID to 12, and user VLAN to 3001. Use traffic profile **ftto_voip**.

```
huawei(config)#service-port vlan 300 gpon 0/1/0 ont 1 gemport 12 multi-
service
user-vlan 3001 tag-transform translate inbound traffic-table name
ftto_voip outboun
d traffic-table name ftto_voip
huawei(config)#service-port vlan 300 gpon 0/1/0 ont 2 gemport 12 multi-
service
user-vlan 3001 tag-transform translate inbound traffic-table name
ftto_voip outboun
d traffic-table name ftto_voip
```

3. Enable the ARP proxy function.

   Voice media streams for different users of the same S-VLAN fail to interchange because the service ports of the smart VLAN are isolated from each other. Therefore, the ARP proxy function needs to be enabled on the OLT.

   ```
   huawei(config)#arp proxy enable
   huawei(config)#interface vlanif 300
   huawei(config-if-vlanif300)#arp proxy enable
   huawei(config-if-vlanif300)#quit
   ```

4. Save the data.

   ```
   huawei(config)#save
   ```

- Configure the ONU on the Web page.

  1. Log in to the Web configuration window.

     a. Configure the IP address of the PC network adapter to be in the same network segment as the IP address of the local maintenance Ethernet port on the ONU (default: **192.168.100.1**).

     b. Open the Web browser, and enter the IP address of the local maintenance Ethernet port of the ONU.

Copyright © Huawei Technologies Co., Ltd.

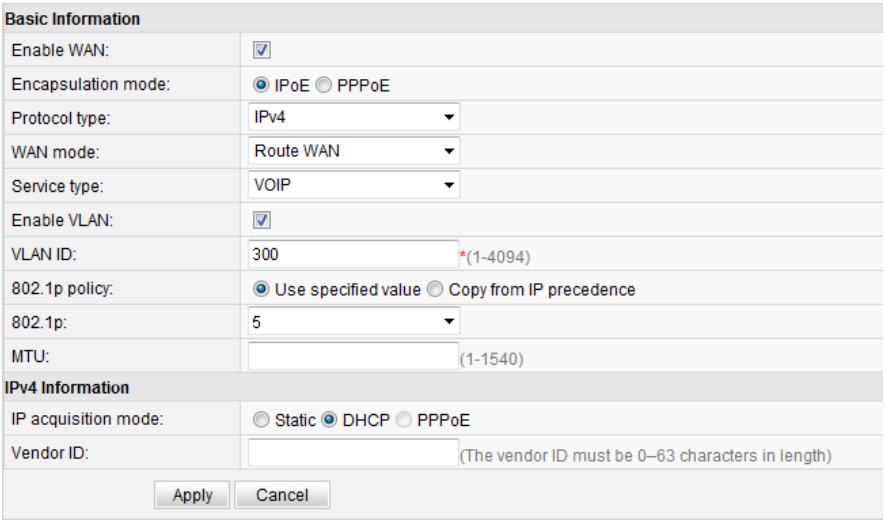
c. On the login window, enter the user name (default: **telecomadmin**) and password (default: **admintelecom**) of the administrator. After the password authentication is passed, the Web configuration interface is displayed.

2. Configure parameters of a voice WAN port.

a. In the navigation tree, choose **WAN** > **WAN Configuration**.

b. In the right pane, click **New**. In the dialog box that is displayed, configure parameters of a WAN port as follows:

- WAN Connection: Enable
- Service List: VoIP (For configuring the VoIP service, VoIP or a combination containing VoIP needs to be selected.)
- Mode: Route
- VLAN ID: 300 (The VLAN ID of the ONU must be the same as the user-side VLAN ID configured on the OLT.)
- 802.1p: 5
- IP Acquisition Mode: DHCP



c. Click **Apply** to apply the configuration.

3. Configure parameters of the SIP-based voice interface.

a. In the navigation tree, choose **Voice** > **VoIP Basic Configuration**.

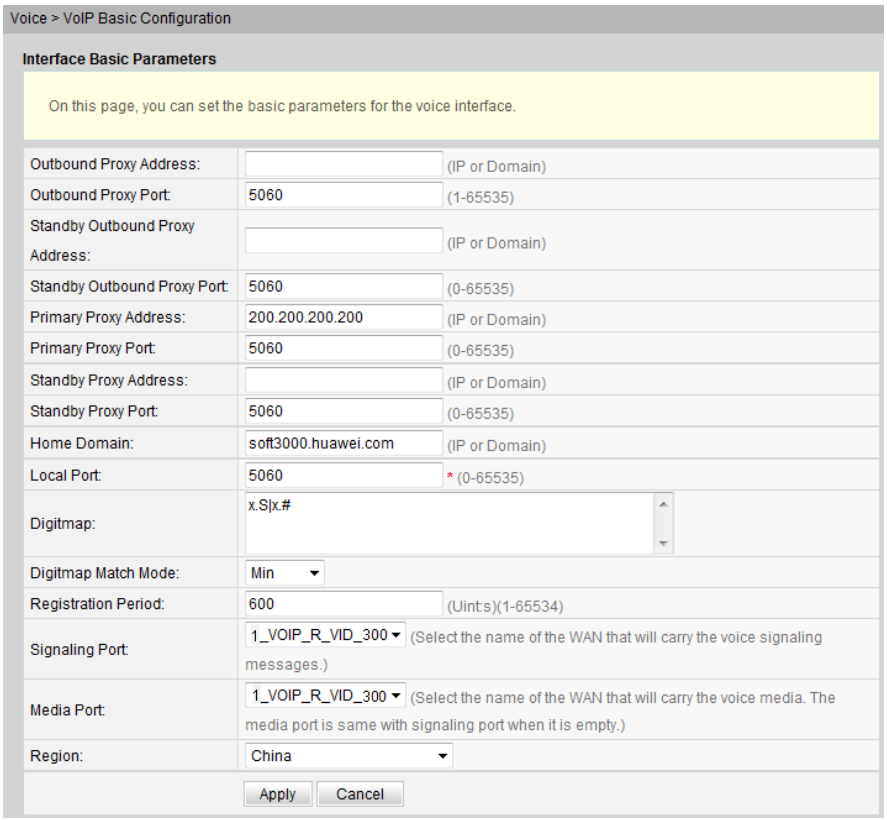
b. In the right pane, configure parameters of the SIP-based voice interface as follows (other parameters use the default settings):

- Set **Proxy Server Address** below **Primary Server** to **200.200.200.200**.
- Home Domain: softx3000.huawei.com
- Signaling Port: 1_VOIP_R_VID_300
- Region: China

Copyright © Huawei Technologies Co., Ltd.

NOTE

- The parameters of the SIP-based voice interface must be consistent with the corresponding configuration on the softswitch.
- If dual-homing is configured, **Proxy Server Address** below **Secondary Server** must be configured.
- If **Signaling Port** is empty, the parameter value is the same as **Media Port**. If the upper-layer network requires isolation of media streams from signaling streams, create different traffic streams for the media streams and signaling streams on the OLT, create different WAN ports on the ONU, and bind the created WAN ports to **Media Port** and **Signaling Port**. When the packet is forwarded from two WAN ports, the configured VLAN is carried by default.



c. Click **Apply** to apply the configuration.

4. Configure parameters of the SIP-based voice users.

a. In the navigation tree, choose **Voice** > **VoIP Basic Configuration**.

b. In the right pane, configure parameters of voice user 1 as follows:

- Register User Name: 80001234
- Auth User Name: 80001234@softx3000.huawei.com
- Password: iadtest1
- Associated POTS: 1 (binding port TEL1 on the ONU)
- Select **Enable** to enable the voice user configuration.

c. Click **Apply** to apply the configuration.

d. Register User Name: 80001235

e. Auth User Name: 80001235@softx3000.huawei.com

Copyright © Huawei Technologies Co., Ltd.

f. Password: iadtest2

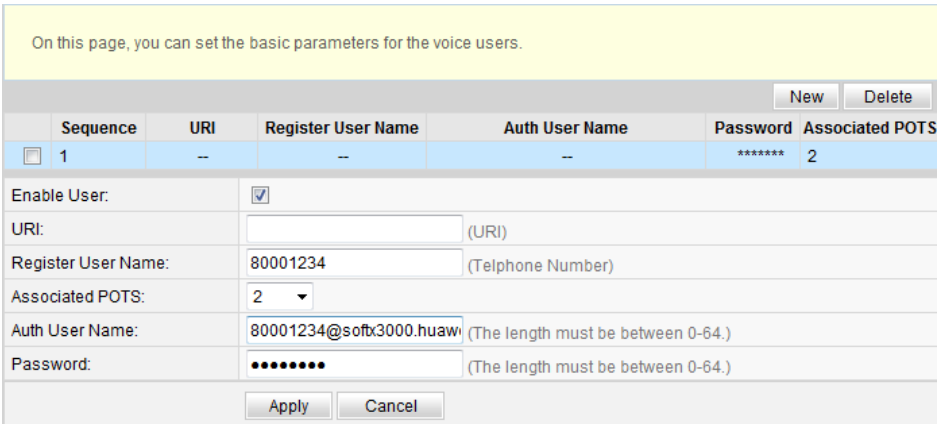
g. Associated POTS: 2 (binding port TEL2 on the ONU)

h. Select **Enable User** to enable the voice user configuration.

i. Click **Apply** to apply the configuration.

NOTE

- The parameters of the SIP-based voice user must be consistent with the corresponding configuration on the softswitch.
- If **Associated POTS** is **1**, port TEL1 on the ONU is bound. If **Associated POTS** is **2**, port TEL2 on the ONU is bound.



5. (Optional) Configure a route.

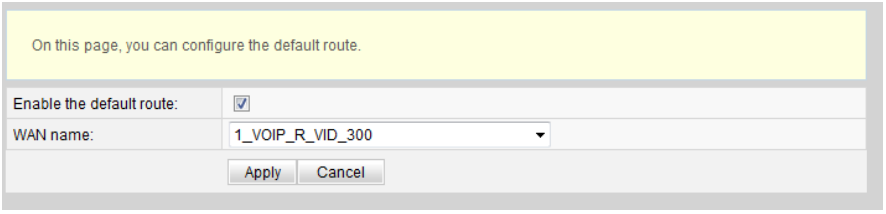
   Perform this operation if the IP address of the ONU and the IP address of the voice server are in different network segments.

   a. Choose **Route** > **Default Route Configuration** from the main menu.

   b. Select **Enable the default route** and set **WAN name** to **1_VOIP_R_VID_300**.

   Figure 12-4 shows the settings.

   Figure 12-4 Configuring a route

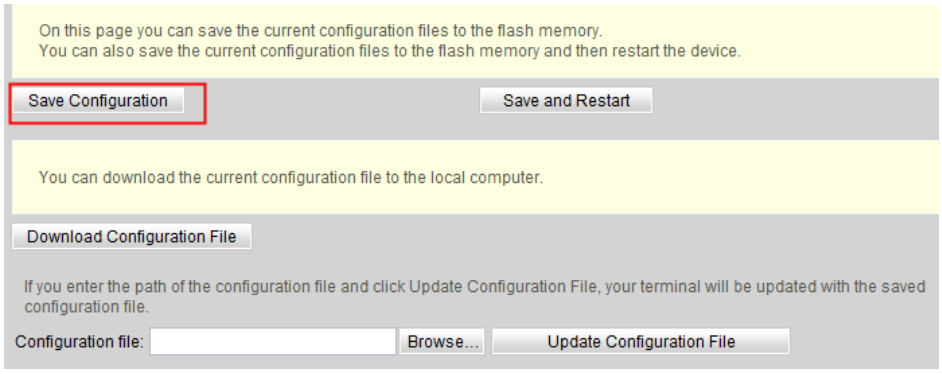
   

   c. Click **Apply** to apply the configuration.

6. Save the configuration.

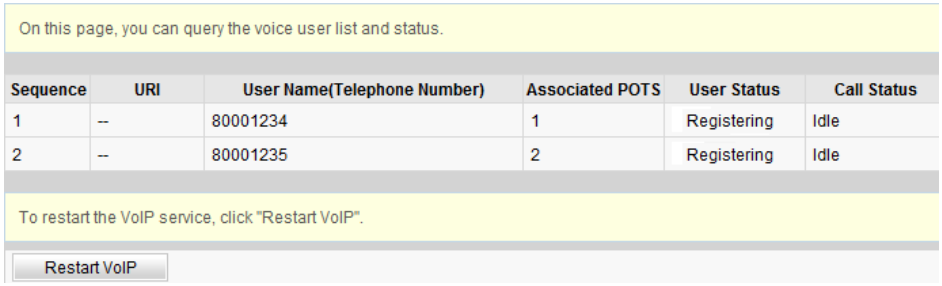
   In the navigation tree, choose **System Tools** > **Configuration File**. In the right pane, click **Save Configuration** to save the configuration.

Copyright © Huawei Technologies Co., Ltd.



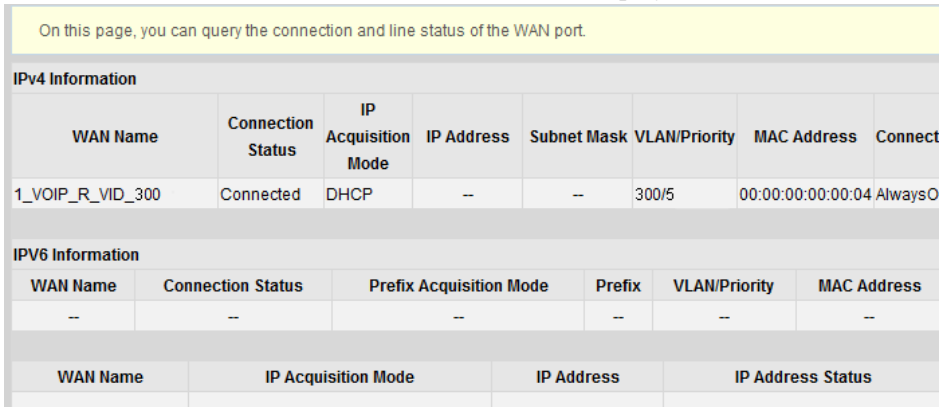
7. Restart the voice process.

   In the navigation tree, choose **Status** > **VoIP Information**. In the right pane, click **Restart VoIP**.



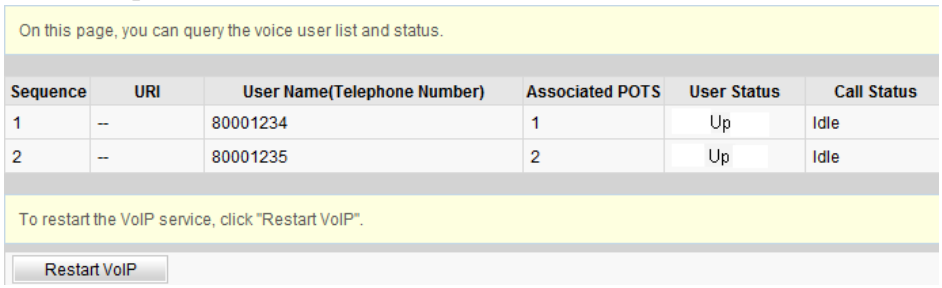
8. Check the ONU connection status.

   In the navigation tree, choose **Status** > **WAN Information**. In the right pane, **Status** is **Connected** and the obtained IP address is displayed at **IP Address**.



9. Check the registration status of the voice user.

   In the navigation tree, choose **Status** > **VoIP Information**. In the right pane, **User Status** is **Up**.



----End

Copyright © Huawei Technologies Co., Ltd.

12.3.8 Configuring the SIP-based Voice Service (Through the CLI)

The OLT manages ONUs and applies VoIP configurations to the ONU using the OMCI protocol. This topic describes how to configure the SIP-based voice service.

Prerequisite

- The SIP interface data and POTS port data corresponding to the MG interface have been configured on the SIP server.
- The connection between the OLT and the SIP server is set up. The OLT can ping the IP address of the SIP server successfully.
- The ONU has been added to the OLT. For details, see **9.7.1.3 Adding an ONT to an OLT**.
- Different voice services require different ONU software versions. Before the configuration, ensure that the current ONU software version supports SIP. For details, see relevant ONU manuals.

Data Plan

Table 12-12 Data plan

Item	Data
ONU line profile	Profile name: ftto_line T-CONT ID: 4 GEM port ID: 12
ONU service profile	Profile name: ftto_ser ONU port capability set: adaptive
Voice parameter	IP address of the SIP server: 200.200.200.200/24 Port ID of the SIP server: 5060 Home domain name: huawei.com User phone number 1: 77730010 User phone number 2: 77730020

Procedure

Step 1 Configure a traffic profile.

Set the profile name to **ftto_voip** and do not limit the upstream and downstream rates. Set the priority to **5** and packets are scheduled according to the priority carried.

Run the **display traffic table ip** command to query existing traffic profiles in the system. If the existing traffic profiles in the system do not meet the requirements, run the **traffic table ip** command to add a traffic profile.

Step 2 Configure the mapping between a GEM port and a VLAN. Create a service VLAN and a service flow.

Copyright © Huawei Technologies Co., Ltd.

Table 12-13 Scenario plan

Scenario	VLAN Plan	VLAN Translation Policy
Scenario 1	Single VLAN tag ● S-VLAN ID: 300 ● S-VLAN type: smart ● S-VLAN attribute: common ● C-VLAN ID: 300	ONU: Configure a VLAN for all ONUs and add the same C-VLAN tag to packets. All ONUs are in the same C-VLAN. OLT: The OLT transparently transmits VLAN tags (the C-VLAN is the same as the planned S-VLAN).
Scenario 2	Single VLAN tag ● S-VLAN ID: 300 ● S-VLAN type: smart ● S-VLAN attribute: common ● C-VLAN ID: 3001	ONU: Configure a VLAN for all ONUs and add the same C-VLAN tag to packets. All ONUs are in the same C-VLAN. OLT: The OLT switches between C-VLAN tags and S-VLAN tags (C-VLAN is different from the planned S-VLAN).

Scenario 1:

Configure the mapping between a GEM port and a VLAN. The service flow of user VLAN 300 is mapped to GEM port 12 in the ONU line profile.

```
huawei(config)#ont-lineprofile gpon profile-name ftto_line
huawei(config-gpon-lineprofile-1)#gem mapping 12 2 vlan 300
huawei(config-gpon-lineprofile-1)#commit
huawei(config-gpon-lineprofile-1)#quit
```

Create a service VLAN and add an upstream port to it. Add upstream port 0/19/0 to VLAN 300.

```
huawei(config)#vlan 300 smart
huawei(config)#port vlan 300 0/19 0
```

Create service flows. Set the service VLAN to 300, GEM port ID to 12, and user VLAN to 300, and use traffic profile **ftto_voip**.

```
huawei(config)#service-port vlan 300 gpon 0/1/0 ont 1 gemport 12 multi-service
 user-vlan 300 inbound traffic-table name ftto_voip outbound traffic-table name
ftto_voip
huawei(config)#service-port vlan 300 gpon 0/1/0 ont 2 gemport 12 multi-service
 user-vlan 300 inbound traffic-table name ftto_voip outbound traffic-table name
ftto_voip
```

Scenario 2:

Configure the mapping between a GEM port and a VLAN. The service flow of user VLAN 3001 is mapped to GEM port 12 in the ONU line profile.

```
huawei(config)#ont-lineprofile gpon profile-name ftto_line
huawei(config-gpon-lineprofile-1)#gem mapping 12 2 vlan 3001
huawei(config-gpon-lineprofile-1)#commit
huawei(config-gpon-lineprofile-1)#quit
```


Copyright © Huawei Technologies Co., Ltd.

Create a service VLAN and add an upstream port to it. Add upstream port 0/19/0 to VLAN 300.

```
huawei(config)#vlan 300 smart
huawei(config)#vlan attrib 300 stacking
huawei(config)#port vlan 300 0/19 0
```

Create service flows. Set the service VLAN to 300, GEM port ID to 12, and user VLAN to 3001. Use traffic profile **ftto_voip**.

```
huawei(config)#service-port vlan 300 gpon 0/1/0 ont 1 gemport 12 multi-service
user-vlan 3001 tag-transform translate inbound traffic-table name ftto_voip
outboun
d traffic-table name ftto_voip
huawei(config)#service-port vlan 300 gpon 0/1/0 ont 2 gemport 12 multi-service
user-vlan 3001 tag-transform translate inbound traffic-table name ftto_voip
outboun
d traffic-table name ftto_voip
```

Step 3 Configure ONU voice service profiles.

ONU voice service profiles include the interface common profile, SIP agent profile, SIP service data profile, POTS port profile, and digitmap profile.

- Interface common profile: saves common attributes of an ONU voice interface, including the fax mode, fax/modem negotiation mode, and priority of the coding and decoding mode.
- SIP agent profile: saves the SIP agent information about an ONU, including the IP address and domain name of the SIP agent server and attributes of media packets and signaling packets.
- SIP service data profile: saves the data information about ONU voice services, including the rights of the call waiting service, three-party service, call forwarding service, and call holding service.
- POTS port profile: saves physical attributes of a POTS port on an ONU, including the impedance, transmitting gain, receiving gain, and signaling type of the POTS port.
- Digitmap profile: saves the digitmap information about an ONU, including the timeout time of the digitmap timer and the digitmap format.

1. Configure an interface common profile.

   Run the **display ont-mg-attribute-profile** command to query the existing interface common profile in the system. If the existing interface common profile in the system does not meet the requirements, run the **ont-mg-attribute-profile add** command to add an interface common profile.

   In this example, the default interface common profile, namely interface common profile 1 is used.

2. Configure an SIP agent profile.

   Run the **display ont-sipagent-profile** command to query the existing SIP agent profile in the system. If the existing SIP agent profile in the system does not meet the requirements, run the **ont-sipagent-profile add** command to add an SIP agent profile.

   Create SIP agent profile 2, set the IP address of the SIP server to 200.200.200.200, and use default values for other parameters.

   ```
   huawei(config)#ont-sipagent-profile add profile-id 2 proxy-server
   200.200.200.200
   ```

3. Configure an SIP service data profile.

   Run the **display ont-siprightflag-profile** command to query the existing SIP agent profile in the system. If the existing SIP service data profile in the system does not meet the requirements, run the **ont-siprightflag-profile add** command to add an SIP service data profile.

Copyright © Huawei Technologies Co., Ltd.

In this example, the default SIP service data profile, namely SIP service data profile 1 is used.

4. Configure a POTS port profile.

   Run the **display ont-pots-profile** command to query the existing POTS port profile in the system. If the existing POTS port profile in the system does not meet the requirements, run the **ont-pots-profile add** command to add a POTS port profile.

   In this example, the default POTS port profile, namely POTS port profile 1 is used.

5. Configure a digitmap profile.

   Run the **display ont-digitmap-profile** command to query the existing digitmap profile in the system. If the existing digitmap profile in the system does not meet the requirements, run the **ont-digitmap-profile add** command to add a digitmap profile.

   In this example, the default digitmap profile, namely digitmap profile 1 is used.

Step 4 Configure an IP address for an ONU SIP user.

For ONU 1 and ONU 2, configure the IP address obtaining mode to the DHCP mode, set the management VLAN to VLAN 20, and use default values for other parameters.

```
huawei(config)#interface gpon 0/1
huawei(config-if-gpon-0/1)#ont ipconfig 0 1 dhcp vlan 20
huawei(config-if-gpon-0/1)#ont ipconfig 0 2 dhcp vlan 20
```

Step 5 Configure SIP POTS users.

1. Add an SIP interface and apply an SIP agent profile to the interface.

   For ONU 1 and ONU 2, set the MG ID to 1, apply SIP agent profile 2 to ONU 1 and ONU 2, and use default values for other parameters.

   If parameters in an SIP agent profile are changed, the SIP agent profile must be reapplied to the ONU so that the changed parameters can take effect.

   ```
   huawei(config-if-gpon-0/1)#if-sip add 0 1 1 sipagent-profile profile-id 2
   huawei(config-if-gpon-0/1)#if-sip add 0 2 1 sipagent-profile profile-id 2
   ```

2. Add POTS users.

   For ONU 1 and ONU 2, set the MG ID to 1 (identical to the MG ID of the added SIP interface), create two POTS users named huawei1 and huawei2, set passwords to user1 and user2, set their phone numbers to 77730010 and 77730020 and use default values for other parameters.

   ```
   huawei(config-if-gpon-0/1)#sippstnuser add 0 1 1 mgid 1 username huawei1 telno
   77730010
   huawei(config-if-gpon-0/1)#sippstnuser add 0 2 1 mgid 1 username huawei2 telno
   77730020
   ```

   Run the **display sippstnuser attribute** command to check whether the configuration of the POTS user is properly set.

   ```
   huawei(config-if-gpon-0/1)#display sippstnuser attribute 0 1 1

   ------------------------------------------------------------------------------
     F/S/P                       : 0/1/0
     ONT ID                      : 1
     Port ID                     : 1

     MG ID                       : 1
     Telephone NO.               : 77730010
     User name                   : huawei1
     Password                    : user1
   ...//The rest of the response information is omitted.

   huawei(config-if-gpon-0/1)#display sippstnuser attribute 0 2 1
   ```


Copyright © Huawei Technologies Co., Ltd.

```
------------------------------------------------------------------------------
  F/S/P                         : 0/1/0
  ONT ID                        : 2
  Port ID                       : 1

  MG ID                         : 1
  Telephone NO.                 : 77730020
  User name                     : huawei2
  Password                      : user2
...//The rest of the response information is omitted.
```

Step 6 Apply and bind an ONU voice service profile to an SIP interface

Currently, the interface common profile, SIP agent profile, SIP service data profile, and POTS port profile can be applied to an SIP interface, and the digitmap profile can be bound to an SIP interface.

For profiles that can be applied to an SIP interface, if parameters in those profiles are changed, those profiles must be reapplied to the SIP interface so that the changed parameters can take effect. For profiles that can be bound to an SIP interface, if parameters in those profiles are changed, those profiles do not need to be rebound to the SIP interface and the changed parameters can take effect.

The method for applying an SIP agent profile is introduced in **Step 5.1**. The following will introduce the methods for applying an interface common profile, an SIP service data profile, and a POTS port profile, and the method for binding a digitmap to an SIP interface.

1. Apply an interface common profile.

   Run the **if-sip attribute** command to apply an interface common profile to an SIP interface or configure the interface customized parameters, or run the **ont-if-sip bat-apply from** command to bulk apply the interface common profiles to SIP interfaces. If you use these two commands to apply the interface common profiles or configure the interface customized parameters repeatedly, the last configurations take effect.

   In this example, the default interface common profile, namely interface common profile 1 is used.

2. Apply an SIP service data profile.

   Run the **sippstnuser rightflag** command to apply an SIP service data profile to an SIP interface or configure the interface customized parameters, or run the **ont-sippstnuser bat-apply from** command to bulk apply the SIP service data profiles to SIP interfaces. If you use these two commands to apply the SIP service data profiles or configure the interface customized parameters repeatedly, the last configurations take effect.

   In this example, the default SIP service data profile, namely SIP service data profile 1 is used.

3. Apply a POTS port profile.

   Run the **pstnport electric** command to apply a POTS port profile to an SIP interface or configure the interface customized parameters, or run the **ont-pstnport electric bat-apply** command to bulk apply the POTS port profiles to SIP interfaces. If you use these two commands to apply the POTS port profiles or configure the interface customized parameters repeatedly, the last configurations take effect.

   In this example, the default POTS port profile, namely POTS port profile 1 is used.

4. Bind a digitmap profile.

   Run the **sippstnuser digitmap** command to bind a digitmap profile to an SIP interface, or run the **ont-sippstnuser bat-bind from** command to bulk apply the digitmap profiles to

Copyright © Huawei Technologies Co., Ltd.

SIP interfaces. If you use these two commands to bind the SIP service data profiles to SIP ports repeatedly, the last configurations take effect.

In this example, the default digitmap profile, namely digitmap profile 1 is used.

Step 7 (Optional) Configure the SIP user codec.

Run the **sippstnuser codec** command to configure the SIP user codec. The SIP user codec will not be configured independently in this example.

Step 8 Save the data.

```
huawei(config)#save
```

----End

12.3.9 Configuring the BTV Service

The OLT is connected to the remote gateway ONU through a GPON port to provide users with the bridge WAN multicast service.

Prerequisites

- The IPTV WAN ports on the ONU use factory defaults.
- The OLT has been connected to the BRAS and the multicast source.
- The ONU has been added to the OLT. For details, see **12.3.3 Adding an ONU to an OLT**.

Data Plan

Table 12-14 Data plan

Item	Data
ONU line profile	Profile name: ftto_line T-CONT ID: 4 GEM port ID: 13
ONU service profile	Profile name: ftto_ser ONU port capability set: adaptive
Traffic profile	ID: 8 802.1p priority: 4 CIR: off (unlimited) Priority-based scheduling policy: local-setting
Multicast service data	Multicast protocol: IGMP proxy Multicast version: IGMPv2 Multicast program: dynamic obtaining mode

Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Configure the OLT.

1. Configure a traffic profile.

   Configure traffic profile 8. Set the CIR to off (unlimited), priority to 4, and priority-based scheduling policy to local-setting (that is, queues are scheduled based on the priority specified in the profile).

   NOTE

   Run the **display traffic table ip** command to query existing traffic profiles in the system. If the existing traffic profiles in the system do not meet the requirements, run the **traffic table ip** command to add a traffic profile.

   ```
   huawei(config)#traffic table ip index 8 cir off priority 4 priority-policy
   local-setting
   ```

2. Configure the VLAN and service flows.

   Table 12-15 Data plan

VLAN Plan	VLAN Translation Policy
Single VLAN tag ● S-VLAN ID: 1000 ● MVLAN ID: 1000 ● VLAN type: smart ● VLAN attribute: common	ONU: duplicates multicast packets based on user ports and MVLANs are stripped off downstream. OLT: duplicates multicast packets based on PON ports with MVLAN unchanged.

   Configure the mapping between a GEM port and an Ethernet port on an ONU. If the ONU is connected to the STB through Ethernet port 2, map the service flow of Ethernet port 2 to GEM port 13 in the ONU line profile.

   ```
   huawei(config)#ont-lineprofile gpon profile-name ftto_line
   huawei(config-gpon-lineprofile-1)#gem mapping 13 2 vlan 1000
   huawei(config-gpon-lineprofile-1)#commit
   huawei(config-gpon-lineprofile-1)#quit
   ```

   Configure the multicast forwarding mode is untagged.

   ```
   huawei(config)#ont-srvprofile gpon profile-name ftto_ser
   huawei(config-gpon-srvprofile-1)#multicast-forward untag
   huawei(config-gpon-srvprofile-1)#commit
   huawei(config-gpon-srvprofile-1)#quit
   ```

   Create a service VLAN and add an upstream port to it. Add upstream port 0/19/0 to VLAN 1000.

   ```
   huawei(config)#vlan 1000 smart
   huawei(config)#port vlan 1000 0/19 0
   ```

   Create service flows. Set the service VLAN to 1000, GEM port ID to 13, and user VLAN to 1000, and use traffic profile 8.

   ```
   huawei(config)#service-port 1 vlan 1000 gpon 0/1/0 ont 1 gemport 13 multi-
   service
    user-vlan 1000 rx-cttr 8 tx-cttr 8
   ```


Copyright © Huawei Technologies Co., Ltd.

```
huawei(config)#service-port 2 vlan 1000 gpon 0/1/0 ont 2 gemport 13 multi-
service
 user-vlan 1000 rx-cttr 8 tx-cttr 8
```

3. Create an MVLAN and configure the IGMP version.

   Set the IGMP version for the MVLAN to IGMPv2.

```
huawei(config)#multicast-vlan 1000
huawei(config-mvlan1000)#igmp version v2
  This operation will delete all IPv4 programs with source IP addresses in the
current multicast VLAN
  Are you sure to change current IGMP version? (y/n)[n]:y
  Command is being executed. Please wait...
  Command has been executed successfully
```

4. Configure a program library.

   Set the mode for obtaining multicast programs to dynamic.

   NOTE

   You can set the mode for obtaining multicast programs to dynamic only when the IGMP mode is off.

```
huawei(config-mvlan1000)#igmp mode off
  Are you sure to close IGMP? (y/n)[n]:y
  Command is being executed. Please wait...
  Command has been executed successfully

huawei(config-mvlan1000)#igmp match mode disable
  Command has been executed successfully
```

   (Optional) Set the address range for the dynamic programs. If you need to limit the address range of dynamic programs, perform this operation. For example, set the address range of dynamic programs to 224.1.1.1-224.1.1.100.

```
huawei(config-mvlan1000)#igmp match group ip 224.1.1.1 to-ip 224.1.1.100
```

5. Set the IGMP mode.

   Select the IGMP proxy mode.

```
huawei(config-mvlan1000)#igmp mode proxy
  Are you sure to change IGMP mode? (y/n)[n]:y
  Command is being executed. Please wait...
  Command has been executed successfully
```

6. Configure the IGMP upstream port.

   Set the IGMP upstream port ID to 0/19/0 and working mode to **default**. Protocol packets are transmitted to all the IGMP upstream ports in the multicast VLAN.

```
huawei(config-mvlan1000)#igmp uplink-port 0/19/0
huawei(config-mvlan1000)#btv
huawei(config-btv)#igmp uplink-port-mode default
Are you sure to change the uplink port mode?(y/n)[n]:y
```

7. (Optional) Set multicast global parameters.

   In this example, the default settings are used for all the multicast global parameters.

8. Configure multicast users.

   Add service ports 1 and 2 as multicast users.

```
huawei(config-btv)#igmp user add service-port 1
huawei(config-btv)#igmp user add service-port 2
huawei(config-btv)#multicast-vlan 1000
huawei(config-mvlan1000)#igmp multicast-vlan member service-port 1
huawei(config-mvlan1000)#igmp multicast-vlan member service-port 2
huawei(config-mvlan1000)#quit
```

9. Save the data.

Copyright © Huawei Technologies Co., Ltd.

```
huawei(config)#save
```

Step 2 The ONU does not need to be configured.

----End

12.3.10 Configuring the VoD Service

The OLT is connected to the remote gateway ONU through a GPON port to provide users with the VoD service.

Prerequisites

- The IPTV WAN ports on the ONU use factory defaults.
- The OLT has been connected to the BRAS and the program source.
- The ONU has been added to the OLT. For details, see **12.3.3 Adding an ONU to an OLT**.

Data Plan

Table 12-16 Data plan

Item	Data
ONU line profile	Profile name: ftto_line T-CONT ID: 4 GEM port ID: 13
ONU service profile	Profile name: ftto_ser ONU port capability set: adaptive
Traffic profile	ID: 8 802.1p priority: 4 CIR: off (unlimited) Priority-based scheduling policy: local-setting

Procedure

Step 1 Configure the OLT.

1. Configure a traffic profile.

   Configure traffic profile 8. Set the CIR to off (unlimited), priority to 4, and priority-based scheduling policy to local-setting (that is, queues are scheduled based on the priority specified in the profile).

   NOTE

   Run the **display traffic table ip** command to query existing traffic profiles in the system. If the existing traffic profiles in the system do not meet the requirements, run the **traffic table ip** command to add a traffic profile.

Copyright © Huawei Technologies Co., Ltd.

```
huawei(config)#traffic table ip index 8 cir off priority 4 priority-policy
local-setting
```

2. Configure the VLAN and service flows.

Table 12-17 Data plan

VLAN Plan	VLAN Translation Policy
Single VLAN tag ● S-VLAN ID: 1100 ● VLAN type: smart ● VLAN attribute: common ● C-VLAN: 2001	The ONU adds CVALN tags to packets: untagged <-> C-VLAN tag. The OLT implements VLAN translation: C-VLAN tag <-> S-VLAN tag.

Configure the mapping between a GEM port and a VLAN. The service flow of user VLAN 2001 is mapped to GEM port 13 in the ONU line profile.

```
huawei(config)#ont-lineprofile gpon profile-name ftto_line
huawei(config-gpon-lineprofile-1)#gem mapping 13 4 vlan 2001
huawei(config-gpon-lineprofile-1)#commit
huawei(config-gpon-lineprofile-1)#quit
```

Create a service VLAN and add an upstream port to it. Add upstream port 0/19/0 to VLAN 1100.

```
huawei(config)#vlan 1100 smart
huawei(config)#port vlan 1100 0/19 0
```

Create service flows. Set the S-VLAN to 1100, GEM port ID to 13, and C-VLAN to 2001, and use traffic profile 8. Set the VLAN translation policy to Translate. The C-VLAN 2001 of the ONU is translated to S-VLAN 1100.

```
huawei(config)#service-port 3 vlan 1100 gpon 0/1/0 ont 1 gemport 13
multi-service user-vlan 2001 tag-transform translate rx-cttr 8 tx-cttr 8
huawei(config)#service-port 4 vlan 1100 gpon 0/1/0 ont 2 gemport 13
multi-service user-vlan 2001 tag-transform translate rx-cttr 8 tx-cttr 8
```

3. Save the data.

```
huawei(config)#save
```

Step 2 The ONU does not need to be configured.

----End

12.3.11 Configuring Link Aggregation, Congestion Control, and Security Policy

Service reliability is improved by configuring uplink aggregation and priority scheduling policy for queues in global configuration mode, and service security is improved by configuring security policy in global configuration mode.

Copyright © Huawei Technologies Co., Ltd.

Context

In link aggregation, multiple uplink Ethernet ports are aggregated into a group to increase bandwidth and reliability of uplinks of the OLT. You are advised to configure link aggregation.

Congestion control queues packets from one port into multiple queues and schedules the packets based on queue priorities. You are advised to configure congestion control.

Security policy involves system security, user security, and service security, ensuring service security from different aspects.

NOTE

- You are advised to enable the service security feature according to service types. For details, see **12.2.6 Principle of Security Data Plan**.
- The configuration of the system security, user security, and service security introduced in this topic is on the OLT side. The configuration on the ONU side is through the web and is simple, here we do not introduced it.

Procedure

- Configure link aggregation.

  On the OLT side, configure upstream ports 0/19/0 and 0/19/1 as an aggregation group. Each member port in the aggregation group is allocated packets based on the source MAC address. The working mode is LACP static aggregation.

  ```
  huawei(config)#link-aggregation 0/19 0-1 ingress workmode lacp-static
  ```

- Configure queue scheduling(On the OLT side).

  According to "**12.2.2 Principle of QoS Planning**", all packets are scheduled in strict priority queue mode and mapped into different queues based on priorities.

  ```
  huawei(config)#queue-scheduler strict-priority
  huawei(config)#cos-queue-map cos0 0 cos4 4 cos5 5 cos6 6
  ```

- Configure system security.
  - Enable deny of service (DoS) anti-attack on the OLT.
    1. Run the **security anti-dos enable** command to globally enable DoS anti-attack.
    2. Run the **security anti-dos control-packet policy** command to configure a protocol packet processing policy that will be used when a DoS attack occurs.
    3. Run the **security anti-dos control-packet rate** command to configure the threshold for the rate of sending protocol packets to the CPU.
  - Enable IP address anti-attack on the OLT.

    Run the **security anti-ipattack enable** command to enable IP address anti-attack.
- Configure user security.
  - Enable MAC address anti-flapping on the OLT.

    Run the **security anti-macduplicate enable** command to enable MAC address anti-flapping.
  - Enable MAC address anti-spoofing on the OLT.
    1. In global config mode, run the **security anti-macspoofing enable** command to globally enable MAC address anti-spoofing.
    2. Enable MAC address anti-spoofing at VLAN level in global config mode or service profile mode:

Copyright © Huawei Technologies Co., Ltd.

a. In global config mode, run the **security anti-macspoofing vlan** command to enable MAC address anti-spoofing.

b. Perform the following operations to enable MAC address anti-spoofing in service profile mode:

a. In global config mode, run the **vlan service-profile** command to create a VLAN service profile.

b. Run the **security anti-macspoofing enable** command to enable MAC address anti-spoofing at VLAN level.

c. Run the **commit** command to make the profile configuration take effect.

d. Run the **quit** command to quit the VLAN service profile mode.

e. Run the **vlan bind service-profile** command to bind the created VLAN service profile to a VLAN.

3. (Optional) Run the **security anti-macspoofing max-mac-count** command to set the maximum number of MAC addresses that can be bound to a service flow.

4. (Optional) Run the **security anti-macspoofing exclude** command to configure the types of packets for which MAC address anti-spoofing does not take effect, such as Internet Group Management Protocol (IGMP) packets.

- Configure service security.
  - Enable Dynamic Host Configuration Protocol (DHCP) Option 82 on the OLT. This configuration is recommended for the DHCP-based Internet access service.

1. DHCP Option 82 can be enabled or disabled at four levels: global, port, VLAN, and service port levels. This function takes effect only after it is enabled at the four levels. Among the four levels, DHCP Option 82 is disabled only at the global level by default.
   - The global level: In global config mode, run the **dhcp option82** command to enable DHCP Option 82 at the global level.

     When you run this command, select the **enable**, **forward**, or **rebuild** parameter based on site requirements. The three parameters can all enable DHCP Option 82 but provide different packet processing policies on the OLT. For details, see the **dhcp option82** command.
   - The port level: In global config mode, run the **dhcp option82 port** or **dhcp option82 board** command to enable DHCP Option 82 at the port level.
   - The VLAN level:

     a. In global config mode, run the **vlan service-profile** command to create a VLAN service profile.

     b. Run the **dhcp option82 enable** command to enable DHCP Option 82 at the VLAN level.

     c. Run the **commit** command to make the profile configuration take effect.

     d. Run the **quit** command to quit the VLAN service profile mode.

     e. Run the **vlan bind service-profile** command to bind the created VLAN service profile to a VLAN.
   - The service port level: In global config mode, run the **dhcp option82 service-port** command to enable DHCP Option 82 at the service port level.

Copyright © Huawei Technologies Co., Ltd.

2. On the OLT, run the **dhcp-option82 permit-forwarding service-port** command with the **enable** parameter selected, to allow ONU DHCP packets to carry Option 82 information.

- Enable Policy Information Transfer Protocol (PITP) on the OLT. This configuration is recommended for the PPPoE-based Internet access service.

  1. PITP can be enabled or disabled at four levels: global, port, VLAN, and service port levels. This function takes effect only after it is enabled at the four levels. Among the four levels, PITP is disabled only at the global level by default.
     - The global level: In global config mode, run the **pitp enable pmode**, **pitp forward pmode**, or **pitp rebuild pmode** command to enable PITP at the global level.

       In the preceding commands, the **enable**, **forward**, and **rebuild** parameters can all enable PITP but provide different packet processing policies on the OLT. Select one of them based on site requirements. For details, see the **pitp** command.
     - The port level: In global config mode, run the **pitp port** or **pitp board** command to enable PITP at the port level.
     - The VLAN level:
       a. In global config mode, run the **vlan service-profile** command to create a VLAN service profile.
       b. Run the **pitp enable** command to enable PITP at the VLAN level.
       c. Run the **commit** command to make the profile configuration take effect.
       d. Run the **quit** command to quit the VLAN service profile mode.
       e. Run the **vlan bind service-profile** command to bind the created VLAN service profile to a VLAN.
     - The service port level: In global config mode, run the **pitp service-port** command to enable PITP at the service port level.
  2. On the OLT, run the **pitp permit-forwarding service-port** command with the **enable** parameter selected, to allow ONU PPPoE packets to carry a vendor tag.

----End

12.3.12 Verifying Services

In the FTTO scenario, ONUs are installed at users' houses or in business buildings which are far away from the central equipment room. ONUs provide remote service verification methods including PPPoE dialup emulation, call emulation, and multicast emulation to facilitate configuration and commissioning engineers to verify services remotely after service configuration.

Prerequisites

ONUs and upper-layer devices have been connected properly. The BRAS and MGC/IMS have been configured.

Copyright © Huawei Technologies Co., Ltd.

Background

Remote Service Verification Method	Function	Description
PPPoE dialup emulation	An ONU simulates a PPPoE user terminal software to perform dialup and interact with the BRAS to verify the connectivity between the ONU and BRAS.	● PPPoE dialup emulation requires a service flow which does not belong to a QinQ VLAN. ● A user name, password, and authentication mode must be configured on the BRAS for the PPPoE dialup emulation. ● An ONU supports a maximum of a PPPoE dialup emulation.
Call Emulation	An ONU simulates a voice user to make a call to check whether the voice service data is correctly configured. You can also use the call emulation function to locate a fault when the voice service is faulty.	● An ONU can simulate a caller or callee to communicate with a phone in a call. In this case, only a functional phone is required in the central office where the acceptance personnel locate. ● An ONU supports only once call emulation.
Multicast emulation	This function enables you to simulate a multicast user going online and lead the program stream to an ONU. You can check whether the multicast service is normal by checking the real-time traffic of the multicast program.	Multicast services configured in the dynamic controllable multicast mode do not support this function.

Data plan

Item	Data	Remarks
PPPoE dialup emulation parameters	PPPoE user name: test@huawei Password: test	The user name, password, and authentication mode for the emulation test must be configured on the BRAS. The entered user name, password, and authentication mode must be consistent with those configured on the BRAS.
Call emulation parameters	ONU POTS ID: 1	The default values are used. You can run the **display pots emulational configuration** command to check the parameter values.

Copyright © Huawei Technologies Co., Ltd.

Item	Data	Remarks
Multicast emulation parameters	Multicast service flow ID: 1 MVLAN: 1000 IP address of the multicast program: 224.1.1.10	-

Procedure

- Verify the Internet access service using PPPoE dialup emulation.
  1. In the xPON board mode, run the **pppoe simulate start** command to start a PPPoE dialup emulation test.

     The service is functional if the test result is **success**. The following test uses GPON as an example:

```
huawei(config)#interface gpon 0/1
huawei(config-if-gpon-0/1)#pppoe simulate start
{ portid<U><0,7> }:0
{ ontid<U><0,127> }:1
{ eth<K>|untagged<K>|vlanid<U><0,4095> }:eth
{ ont-portid<U><1,8> }:4
{ untagged<K>|vlanid<U><0,4095> }:100
{ priority<U><0,7>|user-name<K> }:user-name
{ username<S><Length 1-64> }:test@huawei
{ user-password<K> }:user-password
{ password<S><Length 1-64> }:test
{ authentication-mode<K> }:authentication-mode
{ protocol<E><chap,pap> }:chap

  Command:
          pppoe simulate start 0 1 eth 4 100 user-name test@huawei user-
password
 test authentication-mode chap

huawei(config-if-gpon-0/1)#
  ---------------------------------
  ONT PPPoE Test Result
  ---------------------------------
  F/S/P                : 0/1/0
  ONT-ID               : 1
  ONT ETH Port ID      : 4
  ONT Vlan ID          : 100
  Vlan Priority        : -
  Emluator result      : Success
  Session ID           : 18814
  User IP              : 172.16.100.109
  Gateway IP           : 172.16.100.1
  ---------------------------------
```

- Troubleshooting methods for the Internet access service
  1. Check whether configurations are complete on the OLT.
     - Run the **display ont info** command to query the ONU status to check whether the ONU is registered successfully.
     - Run the **display service-port** command to check whether the Internet access service flow is configured and whether the inner VLAN ID of the service flow is consistent with that in the data plan.

Copyright © Huawei Technologies Co., Ltd.

- If a native VLAN is configured for the Ethernet port on the ONU, run the **display ont port attribute** command in the xPON board mode to check whether the native VLAN is correct.

2. Check the upstream and downstream ports by checking the MAC address learning status.
   a. Run the **display mac-address vlan** command to check the MAC address learning status of the Internet service VLAN.
      - If the upstream port does not learn a MAC address, check the network connections between the upstream port and upper-layer devices and check the configurations of upper-layer devices.
      - If the downstream port does not learn a MAC address, check whether the ONU is activated, whether the PC is connected to the right port on the ONU, and whether the PC is working properly.
   b. Run the **display ont-learned-mac** command to check whether the ONU connecting to the PON port learned any MAC addresses.

      If not, check whether the ONU properly connects to the PC or home gateway (HGW).

- Verify the voice service using call emulation.
  1. Run the **ont emulational call** command to configure a call emulation test.

```
huawei(config)#test
huawei(config-test)#ont emulational call caller-port 0/1/0 1 1 telno
28777192
{ <cr>|caller-stop-time<K> }:

  Command:
          ont emulational call caller-port 0/1/0 1 1 telno 28777192
```

  2. The ONU outputs the call emulation result after the test is complete.

     The service is functional if the test result is **success**.

```
huawei(config-test)#
  ------------------------------------------------------------------
  F/S/P                : 0/1/0
  ONT-ID               : 0
  ONT-POTSID           : 1
  Test type            : caller emulational call test
  Detected number      : 28777192
  Reported number      : 28777192
  Current status       : test end
  Test Result          : success
  ------------------------------------------------------------------
```

- Troubleshooting methods for the voice service.
  1. Check whether configurations are complete on the OLT.
     - Run the **display ont info** command to query the ONU status to check whether the ONU is registered successfully.
     - Run the **display service-port** command to check whether the voice service flow is configured and whether the inner VLAN ID of the service flow is consistent with that in the data plan.
  2. Check the upstream and downstream ports by checking the MAC address learning status.

     Run the **display mac-address vlan** command to check the MAC address learning status of the voice service VLAN.

Copyright © Huawei Technologies Co., Ltd.

- If the upstream port does not learn a MAC address, check the network connections between the upstream port and upper-layer devices and check the configurations of upper-layer devices.
- If the downstream port does not learn a MAC address, check whether the ONU is activated and whether physical links are normal.
- If both the upstream and downstream ports can learn the MAC address, record the MAC address of the ONU and log in to the service router (SR) to check whether an IP address is allocated to the MAC address.

3. Check the registration status of the voice service.
   - You can run the **display ont port state** command on the OLT to query the call connection status on the POTS port. If **Call State** is **RegisterFail** or **Connecting** for a long time, check whether the voice configuration on the MGC/SIP server is consistent with that on the ONU.
   - If the ONU uses the H.248 protocol, you can run the **display ont mg status** command on the OLT to query the registration status of the MG interface that connects to the ONU. If **MG Status** is **UnRegistered** or **Registering** for a long time, check whether the voice configuration on the MGC/SIP server is consistent with that on the ONU.
   - You can query the registration status of the voice service on the ONU web page. If the query result shows that the registration fails or the voice service is in the registering state for a long time, check whether the voice configuration on the MGC/SIP server is consistent with that on the ONU.

- Verify the multicast service using multicast emulation.
  1. Run the **igmp static-join** command to simulate a multicast user to order a multicast program.

     ```
     huawei(config)#btv
     huawei(config-btv)#igmp static-join service-port 1 ip 224.1.1.10 vlan 1000
     ```

     NOTE

     If the multicast program is obtained dynamically, **igmp static-join** can be executed successfully only when the range for obtaining the dynamic program is set.

  2. Run the **display igmp user** command to query the status of the multicast user.

     The multicast user is normal if the queried result is **online**.

     ```
     huawei(config-btv)#display igmp user service-port 1
       User                       : 0/1/0/1
       State                      : online
       Authentication             : no-auth
       Quick leave                : MAC-based
       IGMP flow ID               : 1
       Video flow ID              : 1
       Log switch                 : enable
       Bind profiles              : -
       IGMP version               : IGMP v3
       Current version            : IGMP v3
       Current IGMP IPv6 version  : IGMP IPv6 v2
       Available programs         : 8
       Global leave               : disable
       User max bandwidth         : no-limit
       Used bandwidth(kbps)       : 0
       Used bandwidth
       to max bandwidth(%)        : -
       Total video bandwidth      : -
       Mcast video bandwidth      : -
       Active program list
     ```


Copyright © Huawei Technologies Co., Ltd.

```
------------------------------------------------------------------------
--
  Program name     VLAN  IP/MAC           State           Start time

------------------------------------------------------------------------
--
  PROGRAM-5        1000  224.1.1.10       watching        2011-10-29
                                                         16:33:41+08:00

------------------------------------------------------------------------
--
  Total: 1
```

3. Run the **display multicast flow-statistic** command to query the real-time traffic of the multicast program.

   The multicast program can be ordered if the queried result is a non-empty value.

```
huawei(config-btv)#display multicast flow-statistic vlan 1000 ip
224.1.1.10
{ <cr>|sourceip<K> }:

  Command:
          display multicast flow-statistic vlan 1000 ip 224.1.1.10
  Command is being executed. Please wait...
  Multicast flow statistic result: 8736(kbps)
```

----End

12.4 SME Service Configuration (GPON)

This section describes Internet access, voice, video, and Layer 2 bridging service configurations for small- and medium-sized enterprises (SMEs) in GPON access mode in fiber to the office (FTTO) scenarios.

12.4.1 Bridging and Router Networking

This section describes the configurations for the Internet access, voice, and video services on optical network units (ONUs) in bridging and router networking.

12.4.1.1 Service Requirements and Usage Scenario

Small- and medium-sized enterprise (SME) is positioned for small- and medium-sized enterprises with branches, campuses, and net bars.

Service Requirements

In the SME scenario, optical network units (ONUs) work in bridging mode.

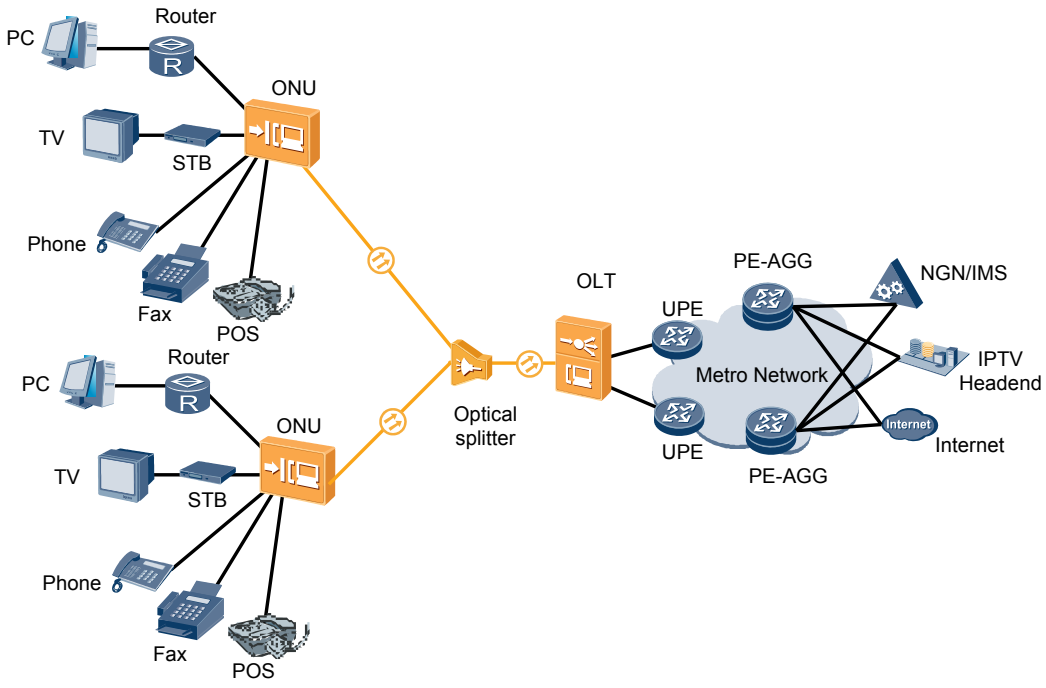
- Users connect to an ONU through an enterprise router. As a Dynamic Host Configuration Protocol (DHCP) client, the router obtains a public IP address through PPPoE dialup. As a DHCP server, the router assigns private IP addresses to the users. After Network Address Translation (NAT), all the users connected to the router use a public IP address to access the Internet. The ONU connects to the optical line terminal (OLT) in GPON access mode and then connects to the upper-layer network, to provide the high-speed Internet access service. The ONU transparently transmits user service flows.

Copyright © Huawei Technologies Co., Ltd.

- Voice service ports connect to phone sets, fax machines, or point of sale (POS) machines.
- TVs connect to an ONU through set top boxes (STBs) to receive VoD and multicast services.
- The Internet access, voice, and IPTV services are secure.
  - The Internet access service is protected against unauthorized access, user account forgery or unauthorized borrowing, MAC or IP address spoofing, and attacks from malicious users.
  - The voice and IPTV services are protected against MAC or IP address spoofing, attacks from malicious users, and heavy traffic.
- A service fault is easy to locate, and services are easy to maintain.

Usage Scenario

Figure 12-5 Bridging and router networking

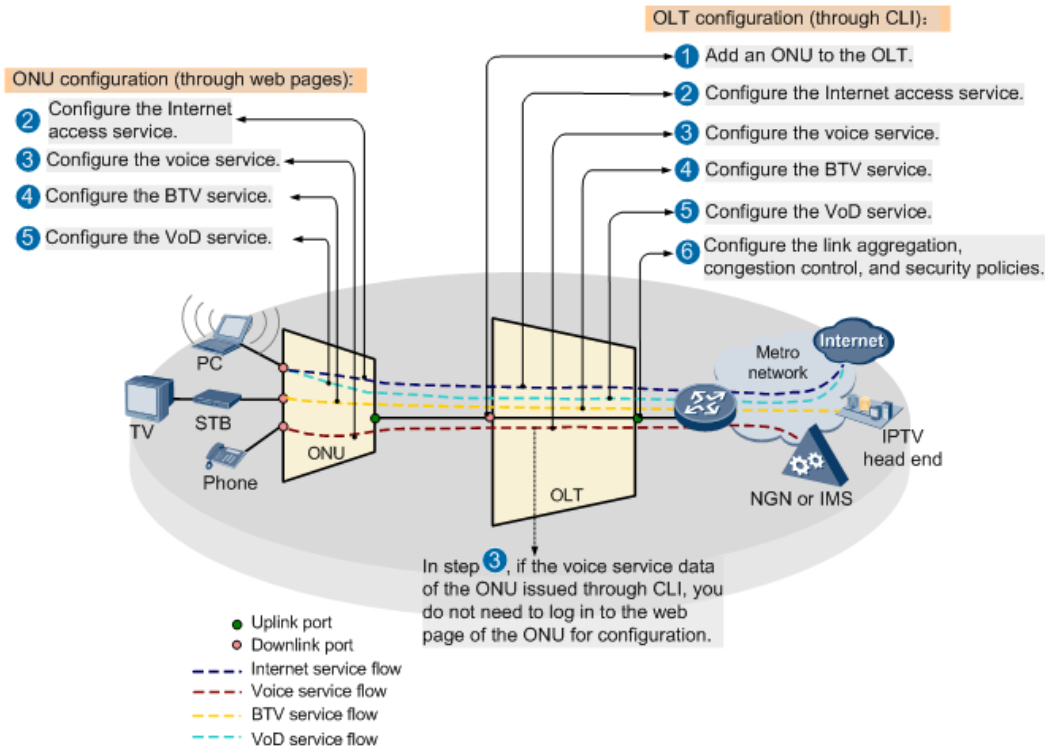


12.4.1.2 Configuration Procedure

Figure 12-6 shows the configuration procedure in the FTTO small- and medium-sized enterprises (SME) scenario.

Copyright © Huawei Technologies Co., Ltd.

Figure 12-6 Configuration procedure in the FTTO SME scenario



The following table lists the detailed description steps.

Item	Procedure		Remarks
OLT	**Adding an ONU to an OLT**		Services can be configured for an ONU only after the ONU is successfully added to an OLT.
OLT ONU	**Configuring the Internet Access Service**		-
OLT ONU	Configuring the Voice Service	**Configuring the H.248-based Voice Service (on a Web Page)**	**NOTE** The H.248 and SIP protocols are mutually exclusive for the VoIP service. Only one of them is configured at a time.
		Configuring the H.248-based Voice Service (Through the CLI)	

Copyright © Huawei Technologies Co., Ltd.

Item	Procedure		Remarks
		Configuring the SIP-based Voice Service (on a Web Page)	
		Configuring the SIP-based Voice Service (Through the CLI)	
OLT	Configuring the BTV Service		IPTV services include the VoD and multicast services that are different in configuration procedures and need to be configured separately.
OLT			
OLT	Configuring Link Aggregation, Congestion Control, and Security Policy		Service reliability is improved by configuring uplink aggregation and priority scheduling policy for queues in global configuration mode, and service security is improved by configuring security policy in global configuration mode.
OLT	Verifying Services		The OLT provides remote verification methods including ONU PPPoE and DHCP dialup emulation and call emulation for configuration and commissioning engineers to verify services remotely after service configuration, avoiding a second on-site operation.

12.4.1.3 Adding an ONU to an OLT

Services can be configured for an ONU only after the ONU is successfully added to an OLT.

Data Plan

Table 12-18 Data plan

Item	Data
DBA profile	Profile name: ftto_dba Profile type: type3 Assured bandwidth: 8 Mbit/s Maximum bandwidth: 50 Mbit/s

Copyright © Huawei Technologies Co., Ltd.

Item	Data
ONU line profile	Profile name: ftto_line T-CONT ID: 4 GEM port ID for management services: 11 GEM port ID for voice services: 12 GEM port ID for video services: 13 GEM port ID for Internet access services: 14
ONU service profile	Profile name: ftto_ser ONU port capability set: adaptive
Network topology data	PON port: 0/1/0 ONU IDs: 1 and 2

Procedure

Step 1 Configure GPON ONU profiles.

GPON ONU profiles include the DBA profile, line profile, service profile, and alarm profile.

- DBA profile: A DBA profile describes GPON traffic parameters. A T-CONT is bound to a DBA profile for dynamic bandwidth allocation, improving upstream bandwidth utilization.
- Line profile: A line profile describes the binding between the T-CONT and the DBA profile, the QoS mode of the traffic stream, and the mapping between the GEM port and the ONU-side service.
- Service profile: A service profile provides the service configuration channel for the ONU that is managed by using optical network terminal management and control interface (OMCI).
- Alarm profile: An alarm profile contains a series of alarm thresholds to measure and monitor the performance of activated ONU lines. When a statistical value reaches the threshold, the host is notified and an alarm is reported to the log host and the NMS.

1. Configure a DBA profile.

   Run the **display dba-profile** command to query existing DBA profiles in the system. If the existing DBA profiles in the system do not meet the requirements, run the **dba-profile add** command to add a DBA profile.

   Create the same DBA profile for different types of services. Set the profile name to **ftto_dba**, profile type to **type3**, assured bandwidth to 8 Mbit/s, and maximum bandwidth to 50 Mbit/s.

   ```
   huawei(config)#dba-profile add profile-name ftto_dba type3 assure 8192 max 51200
   ```

   NOTE

   The DBA implementation is based on an ONU. Therefore, select a DBA profile of the proper bandwidth type and configure proper bandwidth according to the service types and total user count of the ONU. Note that the sum of the fixed bandwidth and the assured bandwidth must not be greater than the total bandwidth of the PON port.

Copyright © Huawei Technologies Co., Ltd.

2. Configure an ONU line profile.

   Create a GPON ONU line profile, named **ftto_line**, and bind it to the DBA profile **ftto_dba**.

   ```
   huawei(config)#ont-lineprofile gpon profile-name ftto_line
   huawei(config-gpon-lineprofile-1)#tcont 4 dba-profile-name ftto_dba
   ```

   Create different GEM ports according to different service types, in which

   - GEM port 11 is used to carry management services.
   - GEM port 12 is used to carry voice services.
   - GEM port 13 is used to carry video services.
   - GEM port 14 is used to carry Internet access services.

   ```
   huawei(config-gpon-lineprofile-1)#gem add 11 eth tcont 4
   huawei(config-gpon-lineprofile-1)#gem add 12 eth tcont 4
   huawei(config-gpon-lineprofile-1)#gem add 13 eth tcont 4
   huawei(config-gpon-lineprofile-1)#gem add 14 eth tcont 4
   ```

   NOTE

   1. To change the default QoS mode, run the **qos-mode** command to set the QoS mode to **gem-car** or **flow-car**, and run the **gem add** command to set the index of the traffic profile bound to the GEM port.
   2. When the QoS mode is priority-queue (PQ), the default queue priority is 0; when the QoS mode is flow-car or gem-car, traffic profile 6 is bound to the GEM port by default (no rate limitation).

   After the configurations are complete, run the **commit** command to apply the parameters settings.

   ```
   huawei(config-gpon-lineprofile-1)#commit
   huawei(config-gpon-lineprofile-1)#quit
   ```

3. Configure an ONU service profile.

   Create a GPON ONU service profile, named **ftto_ser**. Configure the capability set of the ETH port and POTS port to **adaptive**. Then the system automatically adapts to the ONU according to the actual capability of the online ONU.

   ```
   huawei(config)#ont-srvprofile gpon profile-name ftto_ser
   huawei(config-gpon-srvprofile-1)#ont-port eth adaptive pots adaptive
   ```

   After the configurations are complete, run the **commit** command to apply the parameters setting.

   ```
   huawei(config-gpon-srvprofile-1)#commit
   huawei(config-gpon-srvprofile-1)#quit
   ```

4. (Optional) Add an alarm profile.

   - The default GPON alarm profile 1 is used. The alarm thresholds of the default alarm profile are 0, which indicates that no alarm is generated.
   - In this example, the default alarm profile is used, and therefore the configuration of the alarm profile is not required.
   - Run the **gpon alarm-profile add** command to configure a GPON alarm profile, which is used for monitoring the performance of an activated ONU line.

Step 2 Add an ONU.

Connect two ONUs to GPON port 0/1/0. Set the ONU IDs to **1** and **2**, SNs to **32303131D659FD40** and **6877687714852901**, passwords to **0100000001** and **0100000002**, discovery mode for password authentication to **once-on**, and management mode to **OMCI**. Bind the two ONUs to ONU line profile **ftto_line** and ONU service profile **ftto_ser**.

There are two methods of adding an ONU: add an ONU offline and confirm an automatically discovered ONU.

Copyright © Huawei Technologies Co., Ltd.

- Add ONUs offline.

  If the password of an ONU is known, run the **ont add** command to add an ONU offline.

```
huawei(config)#interface gpon 0/1
huawei(config-if-gpon-0/1)#ont add 0 1 password-auth 0100000001 once-on no-aging
omci ont-lineprofile-name
 ftto_line ont-srvprofile-name ftto_ser
huawei(config-if-gpon-0/1)#ont add 0 2 password-auth 0100000002 once-on no-aging
omci ont-lineprofile-name
 ftto_line ont-srvprofile-name ftto_ser
```

- Confirm automatically discovered ONUs

  If the password or SN of an ONU is unknown, run the **port** ***portid*** **ont-auto-find** command in GPON mode to enable the ONU auto-discovery function of the GPON port. Then, run the **ont confirm** command to confirm the ONU.

```
huawei(config)#interface gpon 0/1
huawei(config-if-gpon-0/1)#port 0 ont-auto-find enable
huawei(config-if-gpon-0/1)#display ont autofind 0
  //After this command is executed, the information about all ONUs connected to
the GPON port through optical splitters is displayed.

huawei(config-if-gpon-0/1)#ont confirm 0 ontid 1 sn-auth 32303131D659FD40 omci
ont-lineprofile-name
 ftto_line ont-srvprofile-name ftto_ser
huawei(config-if-gpon-0/1)#ont confirm 0 ontid 2 sn-auth 6877687714852901 omci
ont-lineprofile-name
 ftto_line ont-srvprofile-name ftto_ser
```

  NOTE

  If multiple ONUs of the same type bound to the same line profile or service profile are connected to the same port, you can bulk add ONUs by bulk confirming automatically discovered ONUs to make configuration easier and more efficient. To do so, the preceding command can be modified as follows:

```
huawei(config-if-gpon-0/1)#ont confirm 0 all sn-auth omci ont-lineprofile-name
ftto_line
ont-srvprofile-name ftto_ser
```

- (Optional) Bind the alarm profile to the ONU.

  The default profile 1 is used in this example.

```
huawei(config-if-gpon-0/1)#ont alarm-profile 0 1 profile-id 1
huawei(config-if-gpon-0/1)#ont alarm-profile 0 2 profile-id 1
```

Step 3 Check ONU status.

After an ONU is added, run the **display ont info** command to query the current status of the ONU. Ensure that **Config flag** of the ONU is **active**, **Run State** is **online**, **Config state** is **normal**, and **Match state** is **match**.

```
huawei(config-if-gpon-0/1)#display ont info 0 1
  ------------------------------------------------------------------------
  F/S/P                : 0/1/0
  ONT-ID               : 1
  Control flag         : active    //Indicates that the ONU is
activated.
  Run state            : online    //Indicates that the ONU goes online
successfully.
  Config state         : normal    //Indicates that the configuration state of the
ONU is normal.
  Match state          : match     //Indicates that the capability profile bound to
the ONU is consistent with the actual capability of the ONU.
...//The rest of the response information is omitted.
```

When **Config state** is **failed**, **Run state** is **offline**, or **Match state** is **mismatch**:

- If **Control flag** is **deactive**, run the **ont active** command in GPON mode to activate the ONU.

Copyright © Huawei Technologies Co., Ltd.

- If **Run state** is **offline**, a physical line may be broken or the optical module may be damaged. Check the line and the optical module.
- If **Config state** is **failed**, the configured ONU capability exceeds the actual ONU capability. In this case, run the **display ont failed-configuration** command in the diagnose mode to check the failed configuration item and the failure cause. Then, rectify the fault accordingly.
- If the ONU does not match, that is, **Match state** is **mismatch**, the port types and number of ports undermatch the actual port types and number of ports supported by the ONU. In this case, run the **display ont capability** command to query the actual capability of the ONU, and then select one of the following modes to modify the ONU configuration:
  - Create a proper ONU profile according to the actual capability of the ONU, and then run the **ont modify** command to modify the configuration data of the ONU.
  - Modify the ONU profile according to the actual capability of the ONU and save the modification. Then, the ONU automatically recovers the configuration successfully.

----End

12.4.1.4 Configuring the Internet Access Service

The OLT is connected to the remote ONU through a GPON port to provide users with high-speed Internet access services.

Prerequisite

- The OLT is connected to the BRAS.
- Related configurations are performed on the BRAS according to the authentication and accounting requirements for dialup users. For details about the configuration, see the configuration guide.
- The ONU has been added to the OLT. For details, see **12.4.1.3 Adding an ONU to an OLT** .

Data Plan

Table 12-19 Data plan

Item	Data
ONU line profile	Profile name: ftto_line T-CONT ID: 4 GEM port ID for Internet access service: 14
ONU service profile	Profile name: ftto_ser ONU port capability set: adaptive
Network topology data	Upstream port: 0/19/0 PON port: 0/1/0 ONU IDs: 1 and 2 ID of the port on the ONU that is connected to the PC: 1

Copyright © Huawei Technologies Co., Ltd.

Procedure

- Configure the OLT.
  1. Configure a traffic profile.

     Run the **display traffic table ip** command to query existing traffic profiles in the system. If the traffic profiles existing in the system do not meet the requirements, you need to run the **traffic table ip** command to add a traffic profile.

     Set the profile ID to ftto_hsi, the CIR to 4 Mbit/s, and the priority to 0. In addition, configure the scheduling mode so that packets are scheduled according to their priorities.

     ```
     huawei(config)#traffic table ip name ftto_hsi cir 4096 priority 0 priority-policy local-setting
     ```

  2. Configure the mapping between a GEM port and a VLAN. Create a VLAN and a service flow.

     Table 12-20 Scenario plan

Scenario	VLAN Plan	VLAN Translation Policy
bridging ONU + Router	Double-tagged VLAN ● S-VLAN ID: 100 ● S-VLAN type: smart ● S-VLAN attribute: stacking ● C-VLAN ID: 1001-1002 ● U-VLAN ID: 45	ONU: The upstream packets sent from the router carry C-VLAN tags and the ONU transparently transmits them. OLT: The OLT switches between the U-VLAN tag and the S-VLAN +C-VLAN tag.

     Configure the mapping between a GEM port and a VLAN. The service flow of user-side VLAN 45 is mapped to GEM port 14 in the ONU line profile.

     NOTE

     Here, the user-side VLAN is the VLAN carried by packets sent from HGW to ONU, namely, U-VLAN.

     ```
     huawei(config)#ont-lineprofile gpon profile-name ftto_line
     huawei(config-gpon-lineprofile-1)#gem mapping 14 0 vlan 45
     huawei(config-gpon-lineprofile-1)#commit
     huawei(config-gpon-lineprofile-1)#quit
     ```

     Configure the VLAN of the Ethernet port on the ONU. add Ethernet port 1 to VLAN 45 in the ONU service profile.

     ```
     huawei(config)#ont-srvprofile gpon profile-name ftto_ser
     huawei(config-gpon-srvprofile-1)#port vlan eth 1 45
     huawei(config-gpon-srvprofile-1)#commit
     ```


Copyright © Huawei Technologies Co., Ltd.

Create an Internet access service VLAN and add an upstream port to it. Add upstream port 0/19/0 to VLAN 100.

```
huawei(config)#vlan 100 smart
huawei(config)#vlan attrib 100 stacking
huawei(config)#port vlan 100 0/19 0
```

Create Internet access service flows. Set S-VLAN ID to 100 and GEM port ID to 14. Use traffic profile ftto_hsi.

```
huawei(config)#service-port vlan 100 gpon 0/1/0 ont 1 gemport 14 multi-service
user-vlan 45 tag-transform translate-and-add inner-vlan 1001 inbound traffic-table
 name ftto_hsi outbound traffic-table name ftto_hsi
huawei(config)#service-port vlan 100 gpon 0/1/0 ont 2 gemport 14 multi-service
user-vlan 45 tag-transform translate-and-add inner-vlan 1002 inbound traffic-table
name ftto_hsi outbound traffic-table name ftto_hsi
```

3. Save the data.

```
huawei(config)#save
```

- The ONU does not need to be configured.

----End

12.4.1.5 Configuring the H.248-based Voice Service (on a Web Page)

The OLT is connected to the remote ONU through a GPON port to provide users with the IP-based high-quality and low-cost VoIP service.

Prerequisite

- The interface data and POTS port data corresponding to the MG interface have been configured on the MGC.
- The OLT has been connected to the MGC. The OLT can ping the IP address of the MGC server successfully.
- The ONU has been added to the OLT. For details, see **12.3.3 Adding an ONU to an OLT**.
- Different voice services require different ONU software versions. Before the configuration, ensure that the ONU software version supports H.248. For details, see relevant ONU manuals.

Context

Table 12-21 Data plan

Item	Data
ONU line profile	Profile name: ftto_line T-CONT ID: 4 GEM port ID: 12

Copyright © Huawei Technologies Co., Ltd.

Item	Data
ONU service profile	Profile name: ftto_ser ONU port capability set: adaptive
Networking data	IP address of the MGC server: 200.200.200.200/24 Port ID of the MGC server: 2944

Procedure

- Configure the OLT.
  1. Configure a traffic profile.

     Set the profile name to **ftto_voip** and do not limit the upstream and downstream rates. Set the priority to **5** and packets are scheduled according to the priority carried.

     Run the **display traffic table ip** command to query existing traffic profiles in the system. If the existing traffic profiles in the system do not meet the requirements, run the **traffic table ip** command to add a traffic profile.
  2. Configure the mapping between a GEM port and a VLAN. Create a service VLAN and a service flow.

     Table 12-22 Data plan

Scenario	VLAN Plan	VLAN Translation Policy
Bridging ONU +router	Single VLAN tag ● VLAN ID: 300 ● VLAN type: smart ● VLAN attribute: common ● C-VLAN = S-VLAN	ONU: Provide the VoIP service through the ONU. Configure the service VLAN (S-VLAN) tag in a unified manner. OLT: The OLT transparently transmits S-VLAN tags (the C-VLAN is the same as the planned S-VLAN).

     Configure the mapping between a GEM port and a VLAN. The service flow of user VLAN 300 is mapped to GEM port 12 in the ONU line profile.

     NOTE

     The user VLAN is the VLAN in the packets sent from the router to the ONU, that is, the U-VLAN.

```
huawei(config)#ont-lineprofile gpon profile-name ftto_line
huawei(config-gpon-lineprofile-1)#gem mapping 12 2 vlan 300
huawei(config-gpon-lineprofile-1)#commit
huawei(config-gpon-lineprofile-1)#quit
```

     Configure the VLAN of the Ethernet port on the ONU. If the ONU is connected to the HGW through Ethernet port 1, add Ethernet port 1 to VLAN 45 in the ONU service profile.

Copyright © Huawei Technologies Co., Ltd.

```
huawei(config)#ont-srvprofile gpon profile-name ftth
huawei(config-gpon-srvprofile-1)#port vlan eth 1 45
huawei(config-gpon-srvprofile-1)#commit
huawei(config-gpon-srvprofile-1)#quit
```

Create a service VLAN and add an upstream port to it. Add upstream port 0/19/0 to VLAN 300.

```
huawei(config)#vlan 300 smart
huawei(config)#port vlan 300 0/19 0
```

Create service flows. Set the service VLAN to 300, GEM port ID to 12, and user VLAN to 300, and use traffic profile **ftto_voip**.

```
huawei(config)#service-port vlan 300 gpon 0/1/0 ont 1 gemport 12 multi-
service
 user-vlan 300 inbound traffic-table name ftto_voip outbound traffic-table
name
ftto_voip
huawei(config)#service-port vlan 300 gpon 0/1/0 ont 2 gemport 12 multi-
service
 user-vlan 300 inbound traffic-table name ftto_voip outbound traffic-table
name
ftto_voip
```

3. Enable the ARP proxy function.

   Voice media streams for different users of the same S-VLAN fail to interchange because the service ports of the smart VLAN are isolated from each other. Therefore, the ARP proxy function needs to be enabled on the OLT.

   ```
   huawei(config)#arp proxy enable
   huawei(config)#interface vlanif 300
   huawei(config-if-vlanif300)#arp proxy enable
   huawei(config-if-vlanif300)#quit
   ```

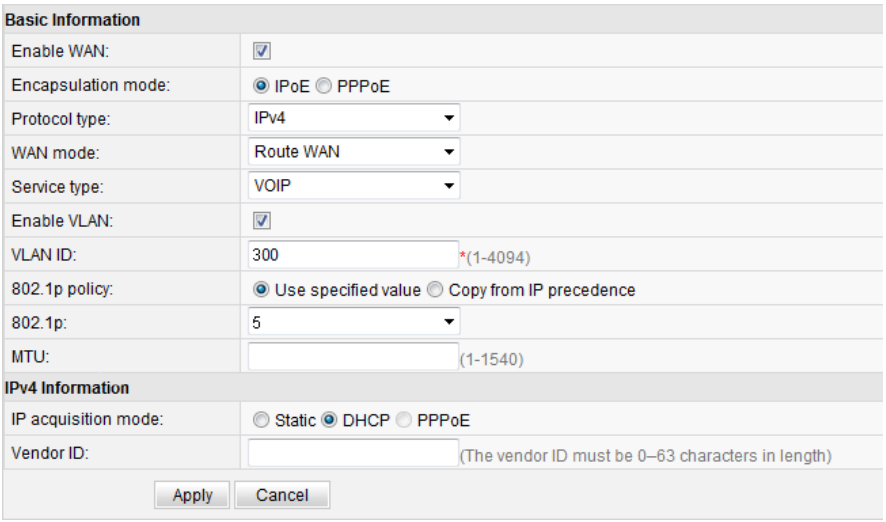
4. Save the data.

   ```
   huawei(config)#save
   ```

- Configure the ONU on the Web page.
  1. Log in to the Web configuration window.
     a. Configure the IP address of the PC network adapter to be in the same network segment as the IP address of the local maintenance Ethernet port on the ONU (default: **192.168.100.1**).
     b. Open the Web browser, and enter the IP address of the local maintenance Ethernet port of the ONU.
     c. On the login window, enter the user name (default: **telecomadmin**) and password (default: **admintelecom**) of the administrator. After the password authentication is passed, the Web configuration interface is displayed.
  2. Configure parameters of a voice WAN port.
     a. In the navigation tree, choose **WAN** > **WAN Configuration**.
     b. In the right pane, click **New**. In the dialog box that is displayed, configure parameters of a WAN port as follows:
        - WAN Connection: Enable
        - Service List: VoIP (For configuring the VoIP service, VoIP or a combination containing VoIP needs to be selected.)
        - Mode: Route

Copyright © Huawei Technologies Co., Ltd.

- VLAN ID: 300 (The VLAN ID of the ONU must be the same as the user-side VLAN ID configured on the OLT.)
- 802.1p: 5
- IP Acquisition Mode: DHCP



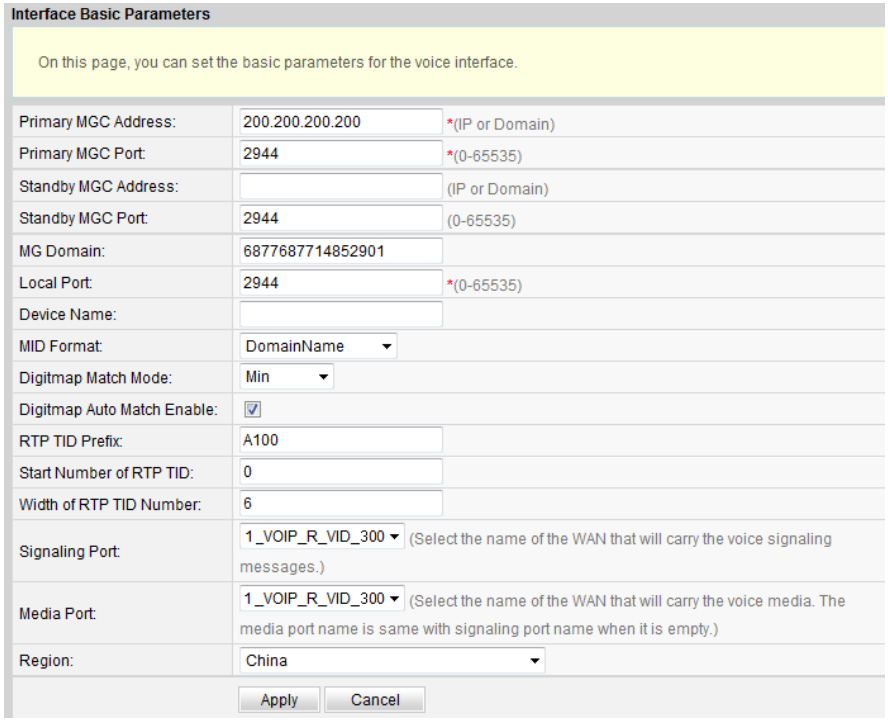
c. Click **Apply** to apply the configuration.

3. Configure the parameters of the H.248-based voice interface.
   a. In the navigation tree, choose **Voice** > **VoIP Basic Configuration**.
   b. In the right pane, configure the parameters of the H.248-based voice interface as follows (other parameters use the default settings):
      - Set **MGC Address** below **Primary Server** to **200.200.200.200**.
      - MID Format: DomainName
      - MG Domain: 6877687714852901
      - Signaling Port: 1_VOIP_R_VID_300
      - Region: China

Copyright © Huawei Technologies Co., Ltd.

NOTE

- The parameters of the H.248-based voice interface must be consistent with the corresponding configuration on the media gateway controller (MGC).
- If dual-homing is configured, **MGC Address** below **Secondary Server** must be configured.
- **MID Format** can be set to **Domain Name**, **IP**, or **Device**. If **MID Format** is set to **Domain Name** or **Device**, the setting must be consistent with the corresponding configuration on the MGC.
- **Domain Name** is ONU's domain name registered with the MGC. It is globally unique. **Domain Name** in this example is ONU's SN.
- If **Media Port** is empty, the parameter value is the same as **Signaling Port**. The media streams are not isolated from signaling streams. If the upper-layer network requires isolation of media streams from signaling streams, create different traffic streams for the media streams and signaling streams on the OLT, create different WAN ports on the ONU, and bind the created WAN ports to **Media Port** and **Signaling Port**.
- **Profile Index** can be set to **Default**, **BT**, **FT**, **KPN**, **PCCW**, **ZTE**, or **BELL**. Choose the value based on the MGC type. **Profile Index** is set to **Default** (indicating interconnection with Huawei MGC) in this example. If the settings do not meet requirements, configure **UserDefine**. For details about how to configure this parameter, contact Huawei technical support engineers.
- When the ONU is interconnected with a third-party softswitch, check **RTP TID Prefix**, **Start Number of RTP TID**, and **Width of RTP TID Number**.



c. Click **Apply** to apply the configuration.

4. Configure parameters of the H.248-based voice users.

a. In the navigation tree, choose **Voice** > **VoIP Basic Configuration**.

b. In the right pane, configure the parameters of voice user 1 as follows:

- Line Name: A0
- Associated POTS: 1 (binding port TEL1 on the ONU)

Copyright © Huawei Technologies Co., Ltd.

- Select **Enable Line Name** to enable the voice user configuration.

c. Click **Apply** to apply the configuration.

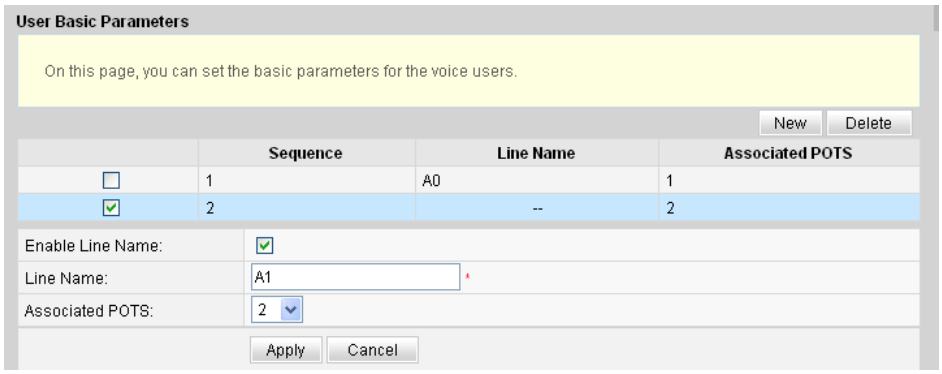
d. In the right pane, click **New** to add voice user 2, and configure the parameters of voice user 2 as follows:

- Line Name: A1
- Associated POTS: 2 (binding port TEL2 on the ONU)
- Select **Enable Line Name** to enable the voice user configuration.

e. Click **Apply** to apply the configuration.

NOTE

- The terminal IDs **A0** and **A1** must be consistent with the corresponding configuration on the MGC.
- If **Associated POTS** is **1**, port TEL1 on the ONU is bound. If **Associated POTS** is **2**, port TEL2 on the ONU is bound.



5. (Optional) Configure a route.

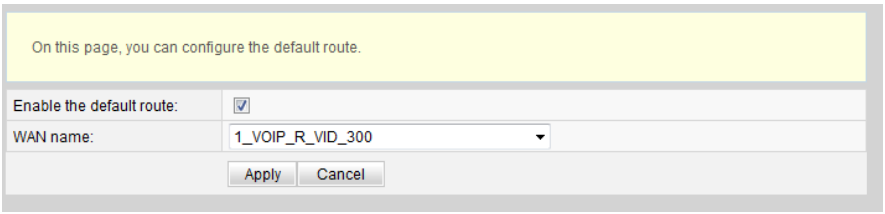
Perform this operation if the IP address of the ONU and the IP address of the voice server are in different network segments.

a. Choose **Route** > **Default Route Configuration** from the main menu.

b. Select **Enable the default route** and set **WAN name** to **1_VOIP_R_VID_300**.

Figure 12-7 shows the settings.

Figure 12-7 Configuring a route

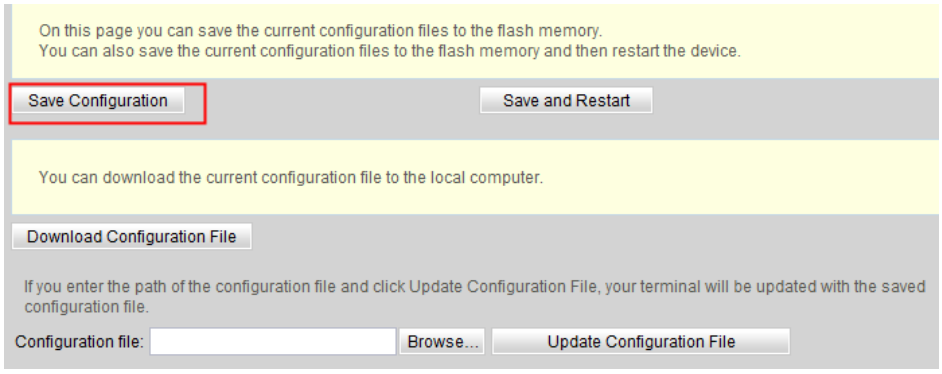


c. Click **Apply** to apply the configuration.

6. Save the configuration.

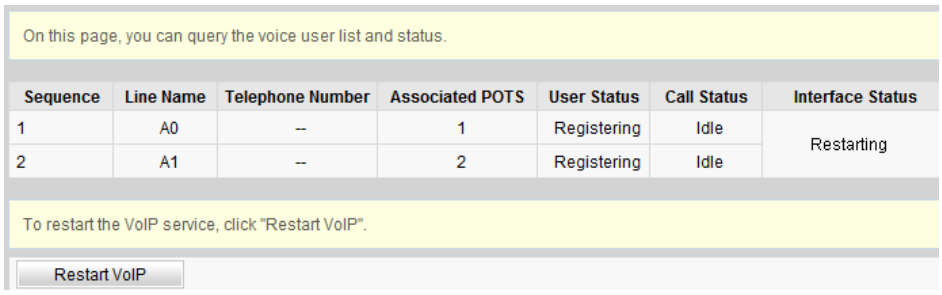
In the navigation tree, choose **System Tools** > **Configuration File**. In the right pane, click **Save Configuration** to save the configuration.

Copyright © Huawei Technologies Co., Ltd.



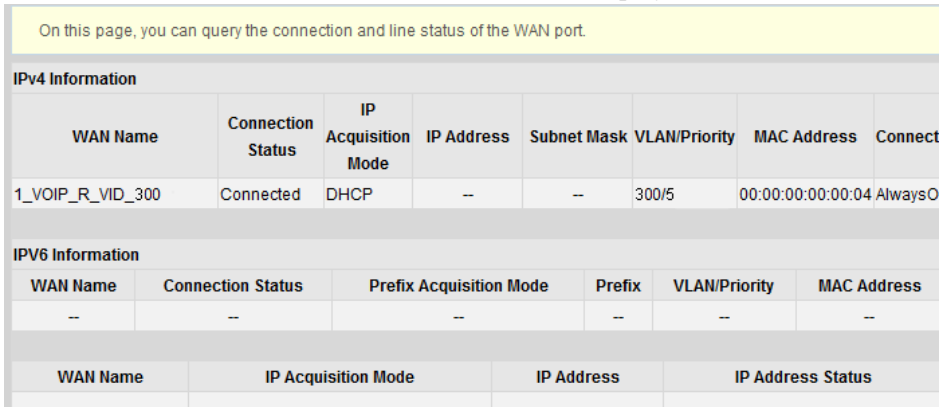
7. Restart the voice process.

   In the navigation tree, choose **Status** > **VoIP Information**. In the right pane, click **Restart VoIP**.



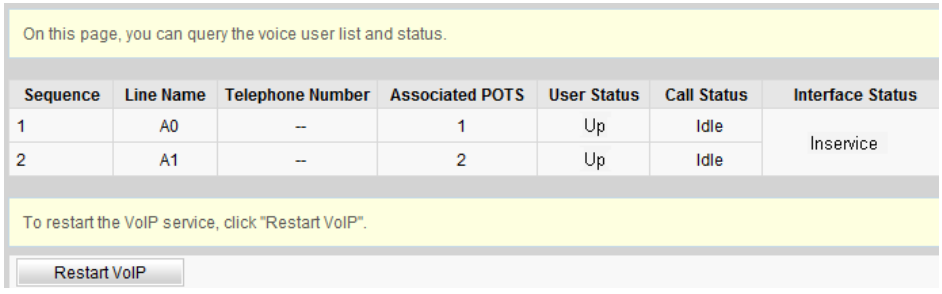
8. Check the ONU connection status.

   In the navigation tree, choose **Status** > **WAN Information**. In the right pane, **Status** is **Connected** and the obtained IP address is displayed at **IP Address**.



9. Check the registration status of a voice user.

   In the navigation tree, choose **Status** > **VoIP Information**. In the right pane, **User Status** is **Up**.



----End

Copyright © Huawei Technologies Co., Ltd.

12.4.1.6 Configuring the H.248-based Voice Service (Through the CLI)

The OLT manages ONUs and applies VoIP configurations to the ONU using the OMCI protocol. This topic describes how to configure the H.248-based voice service.

Prerequisite

- The interface data and POTS port data corresponding to the MG interface have been configured on the MGC.
- The OLT has been connected to the MGC. The OLT can ping the IP address of the MGC server successfully.
- The ONU has been added to the OLT. For details, see **12.3.3 Adding an ONU to an OLT**.
- Different voice services require different ONU software versions. Before the configuration, ensure that the ONU software version supports H.248. For details, see relevant ONU manuals.

Context

Table 12-23 Data plan

Item	Data
ONU line profile	Profile name: ftto_line T-CONT ID: 4 GEM port ID: 12
ONU service profile	Profile name: ftto_ser ONU port capability set: adaptive
Networking data	IP address of the MGC server: 200.200.200.200/24 Port ID of the MGC server: 2944

Procedure

Step 1 Configure a traffic profile.

Set the profile name to **ftto_voip** and do not limit the upstream and downstream rates. Set the priority to **5** and packets are scheduled according to the priority carried.

Run the **display traffic table ip** command to query existing traffic profiles in the system. If the existing traffic profiles in the system do not meet the requirements, run the **traffic table ip** command to add a traffic profile.

Step 2 Configure the mapping between a GEM port and a VLAN. Create a service VLAN and a service flow.

Copyright © Huawei Technologies Co., Ltd.

Table 12-24 Data plan

Scenario	VLAN Plan	VLAN Translation Policy
Bridging ONU +router	Single VLAN tag ● VLAN ID: 300 ● VLAN type: smart ● VLAN attribute: common ● C-VLAN = S-VLAN	ONU: Provide the VoIP service through the ONU. Configure the service VLAN (S-VLAN) tag in a unified manner. OLT: The OLT transparently transmits S-VLAN tags (the C-VLAN is the same as the planned S-VLAN).

Configure the mapping between a GEM port and a VLAN. The service flow of user VLAN 300 is mapped to GEM port 12 in the ONU line profile.

NOTE

The user VLAN is the VLAN in the packets sent from the router to the ONU, that is, the U-VLAN.

```
huawei(config)#ont-lineprofile gpon profile-name ftto_line
huawei(config-gpon-lineprofile-1)#gem mapping 12 2 vlan 300
huawei(config-gpon-lineprofile-1)#commit
huawei(config-gpon-lineprofile-1)#quit
```

Configure the VLAN of the Ethernet port on the ONU. If the ONU is connected to the HGW through Ethernet port 1, add Ethernet port 1 to VLAN 45 in the ONU service profile.

```
huawei(config)#ont-srvprofile gpon profile-name ftth
huawei(config-gpon-srvprofile-1)#port vlan eth 1 45
huawei(config-gpon-srvprofile-1)#commit
huawei(config-gpon-srvprofile-1)#quit
```

Create a service VLAN and add an upstream port to it. Add upstream port 0/19/0 to VLAN 300.

```
huawei(config)#vlan 300 smart
huawei(config)#port vlan 300 0/19 0
```

Create service flows. Set the service VLAN to 300, GEM port ID to 12, and user VLAN to 300, and use traffic profile **ftto_voip**.

```
huawei(config)#service-port vlan 300 gpon 0/1/0 ont 1 gemport 12 multi-service
 user-vlan 300 inbound traffic-table name ftto_voip outbound traffic-table name
ftto_voip
huawei(config)#service-port vlan 300 gpon 0/1/0 ont 2 gemport 12 multi-service
 user-vlan 300 inbound traffic-table name ftto_voip outbound traffic-table name
ftto_voip
```

Step 3 Configure ONU voice service profiles.

ONU voice service profiles include the interface common profile, MGC interface profile, and POTS port profile.

- Interface common profile: saves common attributes of an ONU voice interface, including the fax mode, fax/modem negotiation mode, and priority of the coding and decoding mode.
- MGC interface profile: saves the IP address or domain name of the MGC, protocol port ID of the MGC transport layer to which the MG interface belongs, and DSCP priority of media packets.

Copyright © Huawei Technologies Co., Ltd.

- POTS port profile: saves physical attributes of a POTS port on an ONU, including the impedance, transmitting gain, receiving gain, and signaling type of the POTS port.

1. Configure an interface common profile.

   Run the **display ont-mg-attribute-profile** command to query the existing interface common profile in the system. If the existing interface common profile in the system does not meet the requirements, run the **ont-mg-attribute-profile add** command to add an interface common profile.

   In this example, the default interface common profile, namely interface common profile 1 is used.

2. Configure an MGC interface profile.

   Run the **display ont-mgc-profile** command to query the existing MGC interface profile in the system. If the existing MGC interface profile in the system does not meet the requirements, run the **ont-mgc-profile add** command to add an MGC interface profile.

   Create MGC interface profile 2, set the IP address of the MGC to 200.200.200.200, and use default values for other parameters.

   ```
   huawei(config)#ont-mgc-profile add profile-id 2 primary-mgc 200.200.200.200
   ```

3. Configure a POTS port profile.

   Run the **display ont-pots-profile** command to query the existing POTS port profile in the system. If the existing POTS port profile in the system does not meet the requirements, run the **ont-pots-profile add** command to add a POTS port profile.

   In this example, the default POTS port profile, namely POTS port profile 1 is used.

Step 4 Configure the IP addresses of ONU SIP users.

For ONU 1 and ONU 2, configure the IP address obtaining mode to the static mode, set the IP addresses to 10.10.10.10/24 and 10.10.10.20/24, set the management VLAN to VLAN 20, and use default values for other parameters.

```
huawei(config)#interface gpon 0/1
huawei(config-if-gpon-0/1)#ont ipconfig 0 1 dhcp vlan 20
huawei(config-if-gpon-0/1)#ont ipconfig 0 2 dhcp vlan 20
```

Step 5 Configure H.248 POTS users.

1. Add an H.248 interface and apply an MGC interface profile to the interface.

   For ONU 1 and ONU 2, set the MG ID to 1, apply MGC interface profile 2 to ONU 1 and ONU 2, and use default values for other parameters.

   If parameters of an MGC interface profile are changed, the MGC interface profile must be reapplied to the ONU so that the changed parameters can take effect.

   ```
   huawei(config-if-gpon-0/1)#if-h248 add 0 1 1 mgc-profile profile-id 2
   huawei(config-if-gpon-0/1)#if-h248 add 0 2 1 mgc-profile profile-id 2
   ```

2. Add POTS users.

   For ONU 1 and ONU 2, create a POTS user, set the MG ID to 1 (identical to the MG ID of the H.248 interface), and set the physical terminal port ID to A0 and A1.

   ```
   huawei(config-if-gpon-0/1)#mgpstnuser add 0 1 1 mgid 1 terminalid A0
   huawei(config-if-gpon-0/1)#mgpstnuser add 0 2 1 mgid 1 terminalid A1
   ```

   Run the **display mgpstnuser attribute** command to check whether the configuration of the POTS user is properly set.

   ```
   huawei(config-if-gpon-0/1)#display mgpstnuser attribute 0 1 1

   ---------------------------------------------------------------------------
     F/S/P                       : 0/1/0
   ```


Copyright © Huawei Technologies Co., Ltd.

```
  ONT ID                      : 1
  Port ID                     : 1

  MG ID                       : 1
  Terminal ID                 : A0
...//The rest of the response information is omitted.

huawei(config-if-gpon-0/1)#display mgpstnuser attribute 0 2 1

---------------------------------------------------------------------------
  F/S/P                       : 0/1/0
  ONT ID                      : 2
  Port ID                     : 1

  MG ID                       : 1
  Terminal ID                 : A1
...//The rest of the response information is omitted.
```

Step 6 Apply ONU voice service profiles

After ONU voice service profiles are applied, if parameters in those profiles are changed, those profiles must be reapplied so that the changed parameters can take effect.

1. Apply an interface common profile.

   Run the **if-h248 attribute** command to apply an interface common profile to an H.248 interface or configure the interface customized parameters, or run the **ont-if-h248 bat-apply** command to bulk apply the interface common profiles to H.248 interfaces. If you use these two commands to apply the interface common profiles or configure the interface customized parameters repeatedly, the last configurations take effect.

   In this example, the default interface common profile, namely interface common profile 1 is used.

2. Apply a POTS port profile.

   Run the **pstnport electric** command to apply a POTS port profile to an H.248 interface or configure the interface customized parameters, or run the **ont-pstnport electric bat-apply** command to bulk apply the POTS port profiles to H.248 interfaces. If you use these two commands to apply the POTS port profiles or configure the interface customized parameters repeatedly, the last configurations take effect.

   In this example, the default POTS port profile, namely POTS port profile 1 is used.

Step 7 (Optional) Configure the H.248 user codec.

Run the **mgpstnuser codec** command to configure the H.248 user codec. The H.248 user codec will not be configured independently in this example.

Step 8 Save the data.

```
huawei(config)#save
```

----End

12.4.1.7 Configuring the SIP-based Voice Service (on a Web Page)

The OLT is connected to the remote ONU through a GPON port to provide users with the IP-based high-quality and low-cost VoIP service.

Copyright © Huawei Technologies Co., Ltd.

Prerequisite

- The SIP interface data and POTS port data corresponding to the MG interface have been configured on the SIP server.
- The connection between the OLT and the SIP server is set up. The OLT can ping the IP address of the SIP server successfully.
- The ONU has been added to the OLT. For details, see **9.7.1.3 Adding an ONT to an OLT**.
- Different voice services require different ONU software versions. Before the configuration, ensure that the current ONU software version supports SIP. For details, see relevant ONU manuals.

Data Plan

Table 12-25 Data plan

Item	Data
ONU line profile	Profile name: ftto_line T-CONT ID: 4 GEM port ID: 12
ONU service profile	Profile name: ftto_ser ONU port capability set: adaptive
Voice parameter	IP address of the SIP server: 200.200.200.200/24 Port ID of the SIP server: 5060 Home domain name: huawei.com User phone number 1: 77730010 User phone number 2: 77730020

Procedure

- Configure the OLT.
  1. Configure a traffic profile.

     Set the profile name to **ftto_voip** and do not limit the upstream and downstream rates. Set the priority to **5** and packets are scheduled according to the priority carried.

     Run the **display traffic table ip** command to query existing traffic profiles in the system. If the existing traffic profiles in the system do not meet the requirements, run the **traffic table ip** command to add a traffic profile.
  2. Configure the mapping between a GEM port and a VLAN. Create a service VLAN and a service flow.

Copyright © Huawei Technologies Co., Ltd.

Table 12-26 Data plan

Scenario	VLAN Plan	VLAN Translation Policy
Bridging ONU +router	Single VLAN tag ● VLAN ID: 300 ● VLAN type: smart ● VLAN attribute: common ● C-VLAN = S-VLAN	ONU: Provide the VoIP service through the ONU. Configure the service VLAN (S-VLAN) tag in a unified manner. OLT: The OLT transparently transmits S-VLAN tags (the C-VLAN is the same as the planned S-VLAN).

Configure the mapping between a GEM port and a VLAN. The service flow of user VLAN 300 is mapped to GEM port 12 in the ONU line profile.

NOTE

The user VLAN is the VLAN in the packets sent from the router to the ONU, that is, the U-VLAN.

```
huawei(config)#ont-lineprofile gpon profile-name ftto_line
huawei(config-gpon-lineprofile-1)#gem mapping 12 2 vlan 300
huawei(config-gpon-lineprofile-1)#commit
huawei(config-gpon-lineprofile-1)#quit
```

Configure the VLAN of the Ethernet port on the ONU. If the ONU is connected to the HGW through Ethernet port 1, add Ethernet port 1 to VLAN 45 in the ONU service profile.

```
huawei(config)#ont-srvprofile gpon profile-name ftth
huawei(config-gpon-srvprofile-1)#port vlan eth 1 45
huawei(config-gpon-srvprofile-1)#commit
huawei(config-gpon-srvprofile-1)#quit
```

Create a service VLAN and add an upstream port to it. Add upstream port 0/19/0 to VLAN 300.

```
huawei(config)#vlan 300 smart
huawei(config)#port vlan 300 0/19 0
```

Create service flows. Set the service VLAN to 300, GEM port ID to 12, and user VLAN to 300, and use traffic profile **ftto_voip**.

```
huawei(config)#service-port vlan 300 gpon 0/1/0 ont 1 gemport 12 multi-
service
 user-vlan 300 inbound traffic-table name ftto_voip outbound traffic-table
name
ftto_voip
huawei(config)#service-port vlan 300 gpon 0/1/0 ont 2 gemport 12 multi-
service
 user-vlan 300 inbound traffic-table name ftto_voip outbound traffic-table
name
ftto_voip
```

3. Enable the ARP proxy function.

   Voice media streams for different users of the same S-VLAN fail to interchange because the service ports of the smart VLAN are isolated from each other. Therefore, the ARP proxy function needs to be enabled on the OLT.

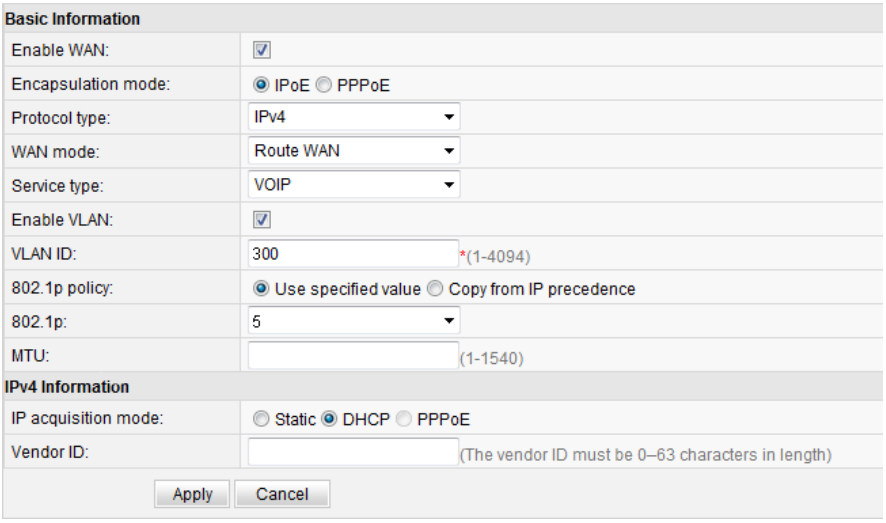
Copyright © Huawei Technologies Co., Ltd.

```
huawei(config)#arp proxy enable
huawei(config)#interface vlanif 300
huawei(config-if-vlanif300)#arp proxy enable
huawei(config-if-vlanif300)#quit
```

4. Save the data.

```
huawei(config)#save
```

- Configure the ONU on the Web page.
  1. Log in to the Web configuration window.
     a. Configure the IP address of the PC network adapter to be in the same network segment as the IP address of the local maintenance Ethernet port on the ONU (default: **192.168.100.1**).
     b. Open the Web browser, and enter the IP address of the local maintenance Ethernet port of the ONU.
     c. On the login window, enter the user name (default: **telecomadmin**) and password (default: **admintelecom**) of the administrator. After the password authentication is passed, the Web configuration interface is displayed.
  2. Configure parameters of a voice WAN port.
     a. In the navigation tree, choose **WAN** > **WAN Configuration**.
     b. In the right pane, click **New**. In the dialog box that is displayed, configure parameters of a WAN port as follows:
        - WAN Connection: Enable
        - Service List: VoIP (For configuring the VoIP service, VoIP or a combination containing VoIP needs to be selected.)
        - Mode: Route
        - VLAN ID: 300 (The VLAN ID of the ONU must be the same as the user-side VLAN ID configured on the OLT.)
        - 802.1p: 5
        - IP Acquisition Mode: DHCP



     c. Click **Apply** to apply the configuration.
  3. Configure parameters of the SIP-based voice interface.

Copyright © Huawei Technologies Co., Ltd.

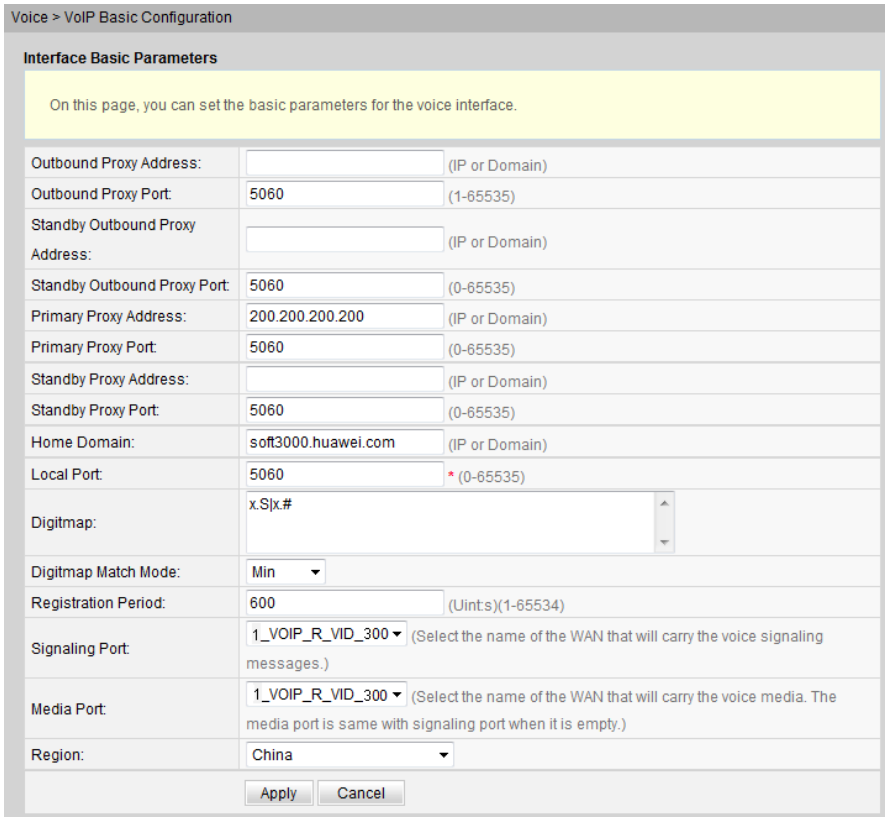
a. In the navigation tree, choose **Voice** > **VoIP Basic Configuration**.

b. In the right pane, configure parameters of the SIP-based voice interface as follows (other parameters use the default settings):

- Set **Proxy Server Address** below **Primary Server** to **200.200.200.200**.
- Home Domain: softx3000.huawei.com
- Signaling Port: 1_VOIP_R_VID_300
- Region: China

NOTE

- The parameters of the SIP-based voice interface must be consistent with the corresponding configuration on the softswitch.
- If dual-homing is configured, **Proxy Server Address** below **Secondary Server** must be configured.
- If **Signaling Port** is empty, the parameter value is the same as **Media Port**. If the upper-layer network requires isolation of media streams from signaling streams, create different traffic streams for the media streams and signaling streams on the OLT, create different WAN ports on the ONU, and bind the created WAN ports to **Media Port** and **Signaling Port**. When the packet is forwarded from two WAN ports, the configured VLAN is carried by default.



c. Click **Apply** to apply the configuration.

4. Configure parameters of the SIP-based voice users.

a. In the navigation tree, choose **Voice** > **VoIP Basic Configuration**.

b. In the right pane, configure parameters of voice user 1 as follows:

- Register User Name: 80001234

Copyright © Huawei Technologies Co., Ltd.

- Auth User Name: 80001234@softx3000.huawei.com
- Password: iadtest1
- Associated POTS: 1 (binding port TEL1 on the ONU)
- Select **Enable** to enable the voice user configuration.

c. Click **Apply** to apply the configuration.

d. Register User Name: 80001235

e. Auth User Name: 80001235@softx3000.huawei.com

f. Password: iadtest2

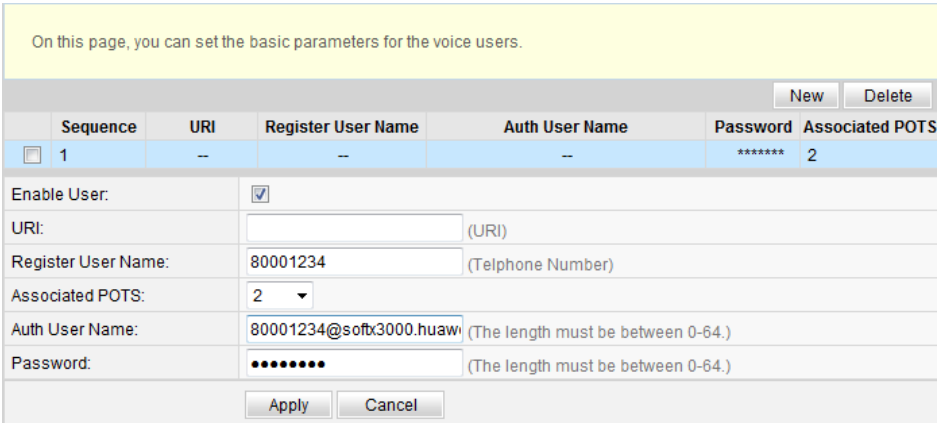
g. Associated POTS: 2 (binding port TEL2 on the ONU)

h. Select **Enable User** to enable the voice user configuration.

i. Click **Apply** to apply the configuration.

NOTE

- The parameters of the SIP-based voice user must be consistent with the corresponding configuration on the softswitch.
- If **Associated POTS** is **1**, port TEL1 on the ONU is bound. If **Associated POTS** is **2**, port TEL2 on the ONU is bound.



5. (Optional) Configure a route.

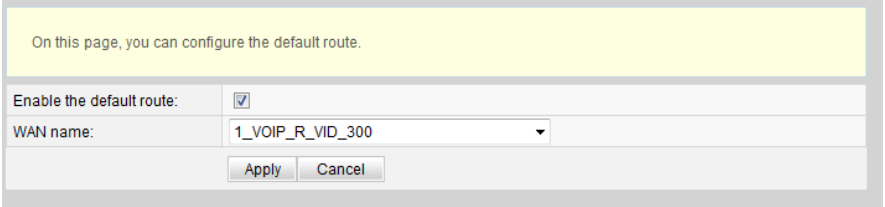
Perform this operation if the IP address of the ONU and the IP address of the voice server are in different network segments.

a. Choose **Route** > **Default Route Configuration** from the main menu.

b. Select **Enable the default route** and set **WAN name** to **1_VOIP_R_VID_300**.

Figure 12-8 shows the settings.

Figure 12-8 Configuring a route

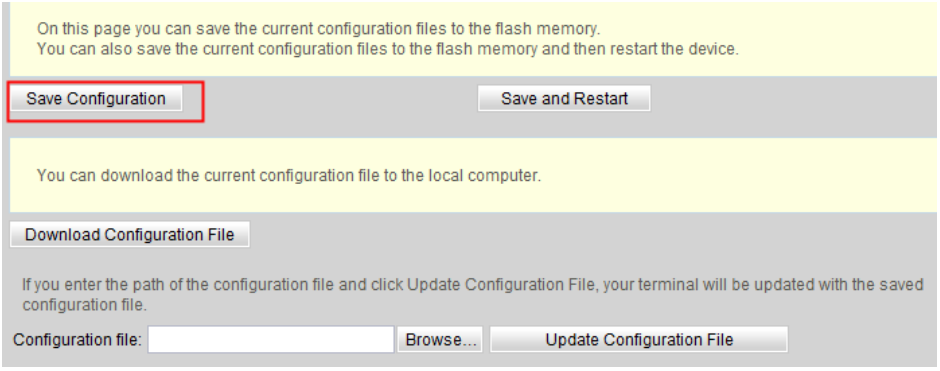


Copyright © Huawei Technologies Co., Ltd.

c. Click **Apply** to apply the configuration.

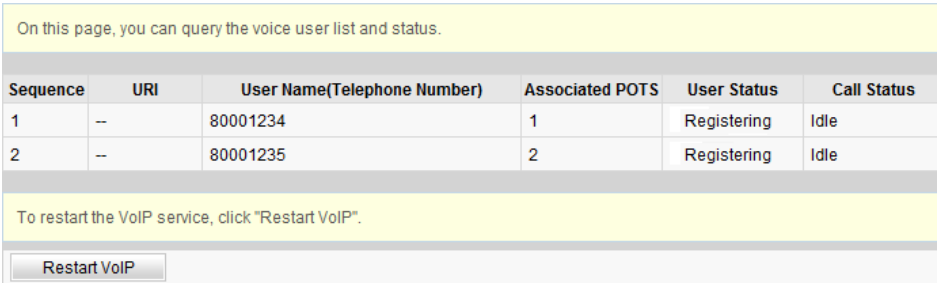
6. Save the configuration.

   In the navigation tree, choose **System Tools** > **Configuration File**. In the right pane, click **Save Configuration** to save the configuration.



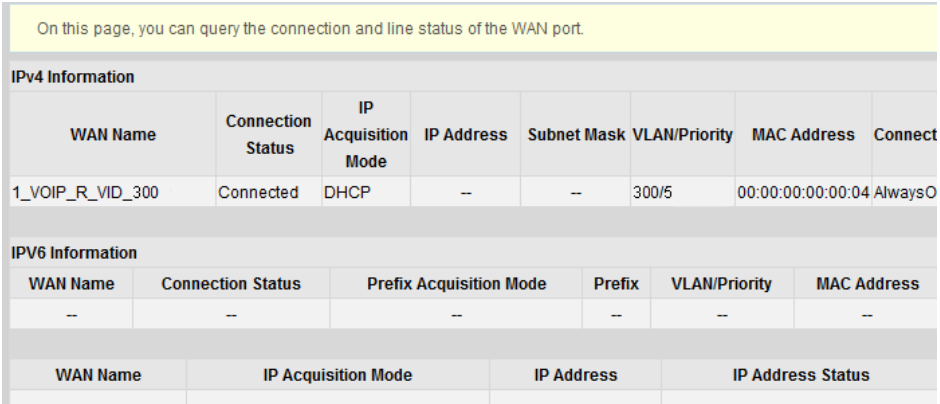
7. Restart the voice process.

   In the navigation tree, choose **Status** > **VoIP Information**. In the right pane, click **Restart VoIP**.



8. Check the ONU connection status.

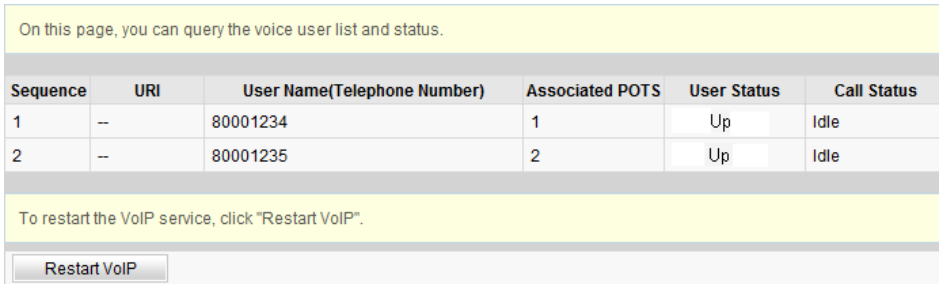
   In the navigation tree, choose **Status** > **WAN Information**. In the right pane, **Status** is **Connected** and the obtained IP address is displayed at **IP Address**.



9. Check the registration status of the voice user.

   In the navigation tree, choose **Status** > **VoIP Information**. In the right pane, **User Status** is **Up**.

Copyright © Huawei Technologies Co., Ltd.



----End

12.4.1.8 Configuring the SIP-based Voice Service (Through the CLI)

The OLT manages ONUs and applies VoIP configurations to the ONU using the OMCI protocol. This topic describes how to configure the SIP-based voice service.

Prerequisite

- The SIP interface data and POTS port data corresponding to the MG interface have been configured on the SIP server.
- The connection between the OLT and the SIP server is set up. The OLT can ping the IP address of the SIP server successfully.
- The ONU has been added to the OLT. For details, see **9.7.1.3 Adding an ONT to an OLT**.
- Different voice services require different ONU software versions. Before the configuration, ensure that the current ONU software version supports SIP. For details, see relevant ONU manuals.

Data Plan

Table 12-27 Data plan

Item	Data
ONU line profile	Profile name: ftto_line T-CONT ID: 4 GEM port ID: 12
ONU service profile	Profile name: ftto_ser ONU port capability set: adaptive
Voice parameter	IP address of the SIP server: 200.200.200.200/24 Port ID of the SIP server: 5060 Home domain name: huawei.com User phone number 1: 77730010 User phone number 2: 77730020

Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Configure the OLT.

1. Configure a traffic profile.

   Set the profile name to **ftto_voip** and do not limit the upstream and downstream rates. Set the priority to **5** and packets are scheduled according to the priority carried.

   Run the **display traffic table ip** command to query existing traffic profiles in the system. If the existing traffic profiles in the system do not meet the requirements, run the **traffic table ip** command to add a traffic profile.

2. Configure the mapping between a GEM port and a VLAN. Create a service VLAN and a service flow.

   Table 12-28 Data plan

Scenario	VLAN Plan	VLAN Translation Policy
Bridging ONU +router	Single VLAN tag ● VLAN ID: 300 ● VLAN type: smart ● VLAN attribute: common ● C-VLAN = S-VLAN	ONU: Provide the VoIP service through the ONU. Configure the service VLAN (S-VLAN) tag in a unified manner. OLT: The OLT transparently transmits S-VLAN tags (the C-VLAN is the same as the planned S-VLAN).

   Configure the mapping between a GEM port and a VLAN. The service flow of user VLAN 300 is mapped to GEM port 12 in the ONU line profile.

   NOTE

   The user VLAN is the VLAN in the packets sent from the router to the ONU, that is, the U-VLAN.

```
huawei(config)#ont-lineprofile gpon profile-name ftto_line
huawei(config-gpon-lineprofile-1)#gem mapping 12 2 vlan 300
huawei(config-gpon-lineprofile-1)#commit
huawei(config-gpon-lineprofile-1)#quit
```

   Configure the VLAN of the Ethernet port on the ONU. If the ONU is connected to the HGW through Ethernet port 1, add Ethernet port 1 to VLAN 45 in the ONU service profile.

```
huawei(config)#ont-srvprofile gpon profile-name ftth
huawei(config-gpon-srvprofile-1)#port vlan eth 1 45
huawei(config-gpon-srvprofile-1)#commit
huawei(config-gpon-srvprofile-1)#quit
```

   Create a service VLAN and add an upstream port to it. Add upstream port 0/19/0 to VLAN 300.

```
huawei(config)#vlan 300 smart
huawei(config)#port vlan 300 0/19 0
```

   Create service flows. Set the service VLAN to 300, GEM port ID to 12, and user VLAN to 300, and use traffic profile **ftto_voip**.

Copyright © Huawei Technologies Co., Ltd.

```
huawei(config)#service-port vlan 300 gpon 0/1/0 ont 1 gemport 12 multi-service
 user-vlan 300 inbound traffic-table name ftto_voip outbound traffic-table
name
ftto_voip
huawei(config)#service-port vlan 300 gpon 0/1/0 ont 2 gemport 12 multi-service
 user-vlan 300 inbound traffic-table name ftto_voip outbound traffic-table
name
ftto_voip
```

3. Enable the ARP proxy function.

   Voice media streams for different users of the same S-VLAN fail to interchange because the service ports of the smart VLAN are isolated from each other. Therefore, the ARP proxy function needs to be enabled on the OLT.

   ```
   huawei(config)#arp proxy enable
   huawei(config)#interface vlanif 300
   huawei(config-if-vlanif300)#arp proxy enable
   huawei(config-if-vlanif300)#quit
   ```

4. Save the data.

   ```
   huawei(config)#save
   ```

Step 2 Configure ONU voice service profiles.

ONU voice service profiles include the interface common profile, SIP agent profile, SIP service data profile, POTS port profile, and digitmap profile.

- Interface common profile: saves common attributes of an ONU voice interface, including the fax mode, fax/modem negotiation mode, and priority of the coding and decoding mode.
- SIP agent profile: saves the SIP agent information about an ONU, including the IP address and domain name of the SIP agent server and attributes of media packets and signaling packets.
- SIP service data profile: saves the data information about ONU voice services, including the rights of the call waiting service, three-party service, call forwarding service, and call holding service.
- POTS port profile: saves physical attributes of a POTS port on an ONU, including the impedance, transmitting gain, receiving gain, and signaling type of the POTS port.
- Digitmap profile: saves the digitmap information about an ONU, including the timeout time of the digitmap timer and the digitmap format.

1. Configure an interface common profile.

   Run the **display ont-mg-attribute-profile** command to query the existing interface common profile in the system. If the existing interface common profile in the system does not meet the requirements, run the **ont-mg-attribute-profile add** command to add an interface common profile.

   In this example, the default interface common profile, namely interface common profile 1 is used.

2. Configure an SIP agent profile.

   Run the **display ont-sipagent-profile** command to query the existing SIP agent profile in the system. If the existing SIP agent profile in the system does not meet the requirements, run the **ont-sipagent-profile add** command to add an SIP agent profile.

   Create SIP agent profile 2, set the IP address of the SIP server to 200.200.200.200, and use default values for other parameters.

   ```
   huawei(config)#ont-sipagent-profile add profile-id 2 proxy-server
   200.200.200.200
   ```

3. Configure an SIP service data profile.

Copyright © Huawei Technologies Co., Ltd.

Run the **display ont-siprightflag-profile** command to query the existing SIP agent profile in the system. If the existing SIP service data profile in the system does not meet the requirements, run the **ont-siprightflag-profile add** command to add an SIP service data profile.

In this example, the default SIP service data profile, namely SIP service data profile 1 is used.

4. Configure a POTS port profile.

   Run the **display ont-pots-profile** command to query the existing POTS port profile in the system. If the existing POTS port profile in the system does not meet the requirements, run the **ont-pots-profile add** command to add a POTS port profile.

   In this example, the default POTS port profile, namely POTS port profile 1 is used.

5. Configure a digitmap profile.

   Run the **display ont-digitmap-profile** command to query the existing digitmap profile in the system. If the existing digitmap profile in the system does not meet the requirements, run the **ont-digitmap-profile add** command to add a digitmap profile.

   In this example, the default digitmap profile, namely digitmap profile 1 is used.

Step 3 Configure an IP address for an ONU SIP user.

For ONU 1 and ONU 2, configure the IP address obtaining mode to the DHCP mode, set the management VLAN to VLAN 20, and use default values for other parameters.

```
huawei(config)#interface gpon 0/1
huawei(config-if-gpon-0/1)#ont ipconfig 0 1 dhcp vlan 20
huawei(config-if-gpon-0/1)#ont ipconfig 0 2 dhcp vlan 20
```

Step 4 Configure SIP POTS users.

1. Add an SIP interface and apply an SIP agent profile to the interface.

   For ONU 1 and ONU 2, set the MG ID to 1, apply SIP agent profile 2 to ONU 1 and ONU 2, and use default values for other parameters.

   If parameters in an SIP agent profile are changed, the SIP agent profile must be reapplied to the ONU so that the changed parameters can take effect.

   ```
   huawei(config-if-gpon-0/1)#if-sip add 0 1 1 sipagent-profile profile-id 2
   huawei(config-if-gpon-0/1)#if-sip add 0 2 1 sipagent-profile profile-id 2
   ```

2. Add POTS users.

   For ONU 1 and ONU 2, set the MG ID to 1 (identical to the MG ID of the added SIP interface), create two POTS users named huawei1 and huawei2, set passwords to user1 and user2, set their phone numbers to 77730010 and 77730020 and use default values for other parameters.

   ```
   huawei(config-if-gpon-0/1)#sippstnuser add 0 1 1 mgid 1 username huawei1 telno
   77730010
   huawei(config-if-gpon-0/1)#sippstnuser add 0 2 1 mgid 1 username huawei2 telno
   77730020
   ```

   Run the **display sippstnuser attribute** command to check whether the configuration of the POTS user is properly set.

   ```
   huawei(config-if-gpon-0/1)#display sippstnuser attribute 0 1 1

   ---------------------------------------------------------------------------
     F/S/P                       : 0/1/0
     ONT ID                      : 1
     Port ID                     : 1

     MG ID                       : 1
   ```


Copyright © Huawei Technologies Co., Ltd.

```
  Telephone NO.               : 77730010
  User name                   : huawei1
  Password                    : user1
...//The rest of the response information is omitted.

huawei(config-if-gpon-0/1)#display sippstnuser attribute 0 2 1

--------------------------------------------------------------------------------
  F/S/P                       : 0/1/0
  ONT ID                      : 2
  Port ID                     : 1

  MG ID                       : 1
  Telephone NO.               : 77730020
  User name                   : huawei2
  Password                    : user2
...//The rest of the response information is omitted.
```

Step 5 Apply and bind an ONU voice service profile to an SIP interface

Currently, the interface common profile, SIP agent profile, SIP service data profile, and POTS port profile can be applied to an SIP interface, and the digitmap profile can be bound to an SIP interface.

For profiles that can be applied to an SIP interface, if parameters in those profiles are changed, those profiles must be reapplied to the SIP interface so that the changed parameters can take effect. For profiles that can be bound to an SIP interface, if parameters in those profiles are changed, those profiles do not need to be rebound to the SIP interface and the changed parameters can take effect.

The method for applying an SIP agent profile is introduced in **Step 4.1**. The following will introduce the methods for applying an interface common profile, an SIP service data profile, and a POTS port profile, and the method for binding a digitmap to an SIP interface.

1. Apply an interface common profile.

   Run the **if-sip attribute** command to apply an interface common profile to an SIP interface or configure the interface customized parameters, or run the **ont-if-sip bat-apply from** command to bulk apply the interface common profiles to SIP interfaces. If you use these two commands to apply the interface common profiles or configure the interface customized parameters repeatedly, the last configurations take effect.

   In this example, the default interface common profile, namely interface common profile 1 is used.

2. Apply an SIP service data profile.

   Run the **sippstnuser rightflag** command to apply an SIP service data profile to an SIP interface or configure the interface customized parameters, or run the **ont-sippstnuser bat-apply from** command to bulk apply the SIP service data profiles to SIP interfaces. If you use these two commands to apply the SIP service data profiles or configure the interface customized parameters repeatedly, the last configurations take effect.

   In this example, the default SIP service data profile, namely SIP service data profile 1 is used.

3. Apply a POTS port profile.

   Run the **pstnport electric** command to apply a POTS port profile to an SIP interface or configure the interface customized parameters, or run the **ont-pstnport electric bat-apply** command to bulk apply the POTS port profiles to SIP interfaces. If you use these two commands to apply the POTS port profiles or configure the interface customized parameters repeatedly, the last configurations take effect.

Copyright © Huawei Technologies Co., Ltd.

In this example, the default POTS port profile, namely POTS port profile 1 is used.

4. Bind a digitmap profile.

   Run the **sippstnuser digitmap** command to bind a digitmap profile to an SIP interface, or run the **ont-sippstnuser bat-bind from** command to bulk apply the digitmap profiles to SIP interfaces. If you use these two commands to bind the SIP service data profiles to SIP ports repeatedly, the last configurations take effect.

   In this example, the default digitmap profile, namely digitmap profile 1 is used.

Step 6 (Optional) Configure the SIP user codec.

Run the **sippstnuser codec** command to configure the SIP user codec. The SIP user codec will not be configured independently in this example.

Step 7 Save the data.

```
huawei(config)#save
```

----End

12.4.1.9 Configuring the BTV Service

The OLT is connected to the remote bridging ONU through a GPON port to provide users with the multicast service.

Prerequisites

- The IPTV WAN ports on the ONU use factory defaults.
- The OLT has been connected to the BRAS and the multicast source.
- The ONU has been added to the OLT. For details, see **12.3.3 Adding an ONU to an OLT**.

Data Plan

Table 12-29 Data plan

Item	Data
ONU line profile	Profile name: ftto_line T-CONT ID: 4 GEM port ID: 13
ONU service profile	Profile name: ftto_ser ONU port capability set: adaptive
Traffic profile	ID: 8 802.1p priority: 4 CIR: off (unlimited) Priority-based scheduling policy: local-setting

Copyright © Huawei Technologies Co., Ltd.

Item	Data
Multicast service data	Multicast protocol: IGMP proxy Multicast version: IGMPv2 Multicast program: dynamic obtaining mode

Procedure

- Configure the OLT.
  1. Configure a traffic profile.

     Configure traffic profile 8. Set the CIR to off (unlimited), priority to 4, and priority-based scheduling policy to local-setting (that is, queues are scheduled based on the priority specified in the profile).

     NOTE

     Run the **display traffic table ip** command to query existing traffic profiles in the system. If the existing traffic profiles in the system do not meet the requirements, run the **traffic table ip** command to add a traffic profile.

     ```
     huawei(config)#traffic table ip index 8 cir off priority 4 priority-policy
     local-setting
     ```

  2. Configure the mapping between a GEM port and an Ethernet port on an ONU. Create a service VLAN and a service flow.

     Table 12-30 Data plan

VLAN Plan	VLAN Translation Policy
● S-VLAN ID: 1000 ● C-VLAN ID: 1000 ● MVLAN ID: 1000 ● VLAN type: smart ● VLAN attribute: common	ONU: transparently transmits the MVLAN of the user port. Multicast packets are duplicated downstream with MVLAN unchanged. OLT: duplicates multicast packets based on PON ports with MVLAN unchanged.

     Configure the mapping between a GEM port and an Ethernet port on an ONU. If the ONU is connected to the STB through Ethernet port 2, map the service flow of Ethernet port 2 to GEM port 13 in the ONU line profile.

     ```
     huawei(config)#ont-lineprofile gpon profile-name ftto_line
     huawei(config-gpon-lineprofile-1)#mapping mode port
     huawei(config-gpon-lineprofile-1)#gem mapping 13 1 eth 2
     huawei(config-gpon-lineprofile-1)#commit
     huawei(config-gpon-lineprofile-1)#quit
     ```

     Configure a VLAN translation policy for the Ethernet port on the ONU. If the ONU is connected to the HGW through Ethernet port 2, VLAN 43 of the HGW is translated to VLAN 1000 and the MVLAN of the ONU is translated to VLAN 1000.

Copyright © Huawei Technologies Co., Ltd.

```
huawei(config)#ont-srvprofile gpon profile-name ftto_ser
huawei(config-gpon-srvprofile-1)#port vlan eth 2 1000
huawei(config-gpon-srvprofile-1)#multicast-forward untag
huawei(config-gpon-srvprofile-1)#commit
huawei(config-gpon-srvprofile-1)#quit
```

Configure the native VLAN of the ONU port. If the ONU is connected to the STB through Ethernet port 2, the native VLAN ID is 1000.

```
huawei(config)#interface gpon 0/1
huawei(config-if-gpon-0/1)#ont port native-vlan 0 1 eth 2 vlan 1000
huawei(config-if-gpon-0/1)#ont port native-vlan 0 2 eth 2 vlan 1000
huawei(config-if-gpon-0/1)#quit
```

Create a service VLAN and add an upstream port to it. Add upstream port 0/19/0 to VLAN 1000.

```
huawei(config)#vlan 1000 smart
huawei(config)#port vlan 1000 0/19 0
```

Create service flows. Set the service VLAN to 1000, GEM port ID to 13, and user VLAN to 1000, and use traffic profile 8.

```
huawei(config)#service-port 1 vlan 1000 gpon 0/1/0 ont 1 gemport 13 multi-
service
 user-vlan 1000 rx-cttr 8 tx-cttr 8
huawei(config)#service-port 2 vlan 1000 gpon 0/1/0 ont 2 gemport 13 multi-
service
 user-vlan 1000 rx-cttr 8 tx-cttr 8
```

3. Create an MVLAN and configure the IGMP version.

   Set the IGMP version for the MVLAN to IGMPv2.

```
huawei(config)#multicast-vlan 1000
huawei(config-mvlan1000)#igmp version v2
  This operation will delete all IPv4 programs with source IP addresses in
the
current multicast VLAN
  Are you sure to change current IGMP version? (y/n)[n]:y
  Command is being executed. Please wait...
  Command has been executed successfully
```

4. Configure a program library.

   Set the mode for obtaining multicast programs to dynamic.

   NOTE

   You can set the mode for obtaining multicast programs to dynamic only when the IGMP mode is off.

```
huawei(config-mvlan1000)#igmp mode off
  Are you sure to close IGMP? (y/n)[n]:y
  Command is being executed. Please wait...
  Command has been executed successfully

huawei(config-mvlan1000)#igmp match mode disable
  Command has been executed successfully
```

   (Optional) Set the address range for the dynamic programs. If you need to limit the address range of dynamic programs, perform this operation. For example, set the address range of dynamic programs to 224.1.1.1-224.1.1.100.

```
huawei(config-mvlan1000)#igmp match group ip 224.1.1.1 to-ip 224.1.1.100
```

5. Set the IGMP mode.

   Select the IGMP proxy mode.

Copyright © Huawei Technologies Co., Ltd.

```
huawei(config-mvlan1000)#igmp mode proxy
  Are you sure to change IGMP mode? (y/n)[n]:y
  Command is being executed. Please wait...
  Command has been executed successfully
```

6. Configure the IGMP upstream port.

   Set the IGMP upstream port ID to 0/19/0 and working mode to **default**. Protocol packets are transmitted to all the IGMP upstream ports in the multicast VLAN.

```
huawei(config-mvlan1000)#igmp uplink-port 0/19/0
huawei(config-mvlan1000)#btv
huawei(config-btv)#igmp uplink-port-mode default
Are you sure to change the uplink port mode?(y/n)[n]:y
```

7. (Optional) Set multicast global parameters.

   In this example, the default settings are used for all the multicast global parameters.

8. Configure multicast users.

   Add service ports 1 and 2 as multicast users.

```
huawei(config-btv)#igmp user add service-port 1
huawei(config-btv)#igmp user add service-port 2
huawei(config-btv)#multicast-vlan 1000
huawei(config-mvlan1000)#igmp multicast-vlan member service-port 1
huawei(config-mvlan1000)#igmp multicast-vlan member service-port 2
huawei(config-mvlan1000)#quit
```

9. Save the data.

```
huawei(config)#save
```

- The ONU does not need to be configured.

----End

12.4.1.10 Configuring the VoD Service

The OLT is connected to the remote bridging ONU through a GPON port to provide users with the VoD service.

Prerequisites

- The OLT is connected to the BRAS and the program source.
- The ONU has been added to the OLT. For details, see **12.3.3 Adding an ONU to an OLT**.

Data Plan

Table 12-31 Data plan

Item	Data
ONU line profile	Profile name: ftto_line T-CONT ID: 4 GEM port ID: 13
ONU service profile	Profile name: ftto_ser ONU port capability set: adaptive

Copyright © Huawei Technologies Co., Ltd.

Item	Data
Traffic profile	ID: 8 802.1p priority: 4 CIR: off (unlimited) Priority-based scheduling policy: local-setting

Procedure

Step 1 Configure the OLT.

1. Configure a traffic profile.

   Configure traffic profile 8. Set the CIR to off (unlimited), priority to 4, and priority-based scheduling policy to local-setting (that is, queues are scheduled based on the priority specified in the profile).

   NOTE

   Run the **display traffic table ip** command to query existing traffic profiles in the system. If the existing traffic profiles in the system do not meet the requirements, run the **traffic table ip** command to add a traffic profile.

   ```
   huawei(config)#traffic table ip index 8 cir off priority 4 priority-policy local-setting
   ```

2. Perform this step in the **bridging ONU+router (single VLAN tag)** scenario.

   Table 12-32 Data plan

VLAN Plan	VLAN Translation Policy
● S-VLAN ID: 1100 ● VLAN type: smart ● VLAN attribute: common ● C-VLAN = U-VLAN	The ONU adds the default C-VLAN tag to packets from iTV service ports. The OLT transparently transmits S-VLAN tags.

   Configure the mapping between a GEM port and a VLAN. The service flow of user VLAN 1100 is mapped to GEM port 13 in the ONU line profile.

   ```
   huawei(config)#ont-lineprofile gpon profile-name ftto_line
   huawei(config-gpon-lineprofile-1)#gem mapping 13 4 vlan 1100
   huawei(config-gpon-lineprofile-1)#commit
   huawei(config-gpon-lineprofile-1)#quit
   ```

   Configure the VLAN of the Ethernet port on the ONU. If the ONU is connected to the STB through Ethernet port 2, add Ethernet port 2 to VLAN 1100.

   ```
   huawei(config)#ont-srvprofile gpon profile-name ftto_ser
   huawei(config-gpon-srvprofile-1)#port vlan eth 2 1100
   huawei(config-gpon-srvprofile-1)#commit
   huawei(config-gpon-srvprofile-1)#quit
   ```


Copyright © Huawei Technologies Co., Ltd.

Create a service VLAN and add an upstream port to it. Add upstream port 0/19/0 to VLAN 1100.

```
huawei(config)#vlan 1100 smart
huawei(config)#port vlan 1100 0/19 0
```

Create service flows. Set the service VLAN to 1100, GEM port ID to 13, and user VLAN to 43, and use traffic profile 8.

```
huawei(config)#service-port 3 vlan 1100 gpon 0/1/0 ont 1 gemport 13
rx-cttr 8 tx-cttr 8 tag-transform transparent
huawei(config)#service-port 4 vlan 1100 gpon 0/1/0 ont 2 gemport 13
rx-cttr 8 tx-cttr 8 tag-transform transparent
```

3. Perform this step in the **bridging ONU+router (double VLAN tags)** scenario.

Table 12-33 Data plan

VLAN Plan	VLAN Translation Policy
● S-VLAN ID: 1100 ● VLAN type: smart ● VLAN attribute: stacking ● C'-VLAN: 2010 ● C-VLAN: 2001	The ONU adds C-VLAN tags to packets. All ONUs are in the same C-VLAN. The OLT switches between the C-VLAN tag and the S-VLAN+C'-VLAN tag.

Configure the mapping between a GEM port and a VLAN. The service flow of user VLAN 2001 is mapped to GEM port 13 in the ONU line profile.

```
huawei(config)#ont-lineprofile gpon profile-name ftto_line
huawei(config-gpon-lineprofile-1)#gem mapping 13 4 vlan 2001
huawei(config-gpon-lineprofile-1)#commit
huawei(config-gpon-lineprofile-1)#quit
```

Configure the VLAN of the Ethernet port on the ONU. If the ONU is connected to the STB through Ethernet port 2, add Ethernet port 2 to VLAN 2001.

```
huawei(config)#ont-srvprofile gpon profile-name ftto_ser
huawei(config-gpon-srvprofile-1)#port vlan eth 2 2001
huawei(config-gpon-srvprofile-1)#commit
huawei(config-gpon-srvprofile-1)#quit
```

Create a service VLAN and add an upstream port to it. Set the attribute of VLAN 1100 to stacking. Add upstream port 0/19/0 to VLAN 1100.

```
huawei(config)#vlan 1100 smart
huawei(config)#vlan attrib 1100 stacking
huawei(config)#port vlan 1100 0/19 0
```

Create service flows. Set the service VLAN to 1100, GEM port ID to 13, and user VLAN to 2001, and use traffic profile 8. Set the VLAN translation policy to Translate and Add to translate the C-VLAN 2001 to C'-VLAN 2010.

```
huawei(config)#service-port 3 vlan 1100 gpon 0/1/0 ont 1 gemport 13
multi-service user-vlan 2001 tag-transform translate-and-add inner-vlan 2010
rx-cttr 8 tx-cttr 8
huawei(config)#service-port 4 vlan 1100 gpon 0/1/0 ont 2 gemport 13
```


Copyright © Huawei Technologies Co., Ltd.

```
multi-service user-vlan 2001 tag-transform translate-and-add inner-vlan 2010
rx-cttr 8 tx-cttr 8
```

4. Save the data.

```
huawei(config)#save
```

Step 2 The ONU does not need to be configured.

----End

12.4.1.11 Configuring Link Aggregation, Congestion Control, and Security Policy

Service reliability is improved by configuring uplink aggregation and priority scheduling policy for queues in global configuration mode, and service security is improved by configuring security policy in global configuration mode.

Context

In link aggregation, multiple uplink Ethernet ports are aggregated into a group to increase bandwidth and reliability of uplinks of the OLT. You are advised to configure link aggregation.

Congestion control queues packets from one port into multiple queues and schedules the packets based on queue priorities. You are advised to configure congestion control.

Security policy involves system security, user security, and service security, ensuring service security from different aspects.

NOTE

- You are advised to enable the service security feature according to service types. For details, see **12.2.6 Principle of Security Data Plan**.
- The configuration of the system security, user security, and service security introduced in this topic is on the OLT side. The configuration on the ONU side is through the web and is simple, here we do not introduced it.

Procedure

- Configure link aggregation.

  On the OLT side, configure upstream ports 0/19/0 and 0/19/1 as an aggregation group. Each member port in the aggregation group is allocated packets based on the source MAC address. The working mode is LACP static aggregation.

```
huawei(config)#link-aggregation 0/19 0-1 ingress workmode lacp-static
```

- Configure queue scheduling(On the OLT side).

  According to "**12.2.2 Principle of QoS Planning**", all packets are scheduled in strict priority queue mode and mapped into different queues based on priorities.

```
huawei(config)#queue-scheduler strict-priority
huawei(config)#cos-queue-map cos0 0 cos4 4 cos5 5 cos6 6
```

- Configure system security.
  - Enable deny of service (DoS) anti-attack on the OLT.
    1. Run the **security anti-dos enable** command to globally enable DoS anti-attack.
    2. Run the **security anti-dos control-packet policy** command to configure a protocol packet processing policy that will be used when a DoS attack occurs.
    3. Run the **security anti-dos control-packet rate** command to configure the threshold for the rate of sending protocol packets to the CPU.

Copyright © Huawei Technologies Co., Ltd.

- Enable IP address anti-attack on the OLT.

  Run the **security anti-ipattack enable** command to enable IP address anti-attack.

- Configure user security.
  - Enable MAC address anti-flapping on the OLT.

    Run the **security anti-macduplicate enable** command to enable MAC address anti-flapping.
  - Enable MAC address anti-spoofing on the OLT.

    1. In global config mode, run the **security anti-macspoofing enable** command to globally enable MAC address anti-spoofing.
    2. Enable MAC address anti-spoofing at VLAN level in global config mode or service profile mode:

       a. In global config mode, run the **security anti-macspoofing vlan** command to enable MAC address anti-spoofing.

       b. Perform the following operations to enable MAC address anti-spoofing in service profile mode:

          a. In global config mode, run the **vlan service-profile** command to create a VLAN service profile.

          b. Run the **security anti-macspoofing enable** command to enable MAC address anti-spoofing at VLAN level.

          c. Run the **commit** command to make the profile configuration take effect.

          d. Run the **quit** command to quit the VLAN service profile mode.

          e. Run the **vlan bind service-profile** command to bind the created VLAN service profile to a VLAN.

    3. (Optional) Run the **security anti-macspoofing max-mac-count** command to set the maximum number of MAC addresses that can be bound to a service flow.
    4. (Optional) Run the **security anti-macspoofing exclude** command to configure the types of packets for which MAC address anti-spoofing does not take effect, such as Internet Group Management Protocol (IGMP) packets.

- Configure service security.
  - Enable Dynamic Host Configuration Protocol (DHCP) Option 82 on the OLT. This configuration is recommended for the DHCP-based Internet access service.

    1. DHCP Option 82 can be enabled or disabled at four levels: global, port, VLAN, and service port levels. This function takes effect only after it is enabled at the four levels. Among the four levels, DHCP Option 82 is disabled only at the global level by default.
       - The global level: In global config mode, run the **dhcp option82** command to enable DHCP Option 82 at the global level.

         When you run this command, select the **enable**, **forward**, or **rebuild** parameter based on site requirements. The three parameters can all enable DHCP Option 82 but provide different packet processing policies on the OLT. For details, see the **dhcp option82** command.

Copyright © Huawei Technologies Co., Ltd.

- The port level: In global config mode, run the **dhcp option82 port** or **dhcp option82 board** command to enable DHCP Option 82 at the port level.
- The VLAN level:
  a. In global config mode, run the **vlan service-profile** command to create a VLAN service profile.
  b. Run the **dhcp option82 enable** command to enable DHCP Option 82 at the VLAN level.
  c. Run the **commit** command to make the profile configuration take effect.
  d. Run the **quit** command to quit the VLAN service profile mode.
  e. Run the **vlan bind service-profile** command to bind the created VLAN service profile to a VLAN.
- The service port level: In global config mode, run the **dhcp option82 service-port** command to enable DHCP Option 82 at the service port level.

2. On the OLT, run the **dhcp-option82 permit-forwarding service-port** command with the **enable** parameter selected, to allow ONU DHCP packets to carry Option 82 information.

- Enable Policy Information Transfer Protocol (PITP) on the OLT. This configuration is recommended for the PPPoE-based Internet access service.

1. PITP can be enabled or disabled at four levels: global, port, VLAN, and service port levels. This function takes effect only after it is enabled at the four levels. Among the four levels, PITP is disabled only at the global level by default.
   - The global level: In global config mode, run the **pitp enable pmode**, **pitp forward pmode**, or **pitp rebuild pmode** command to enable PITP at the global level.

     In the preceding commands, the **enable**, **forward**, and **rebuild** parameters can all enable PITP but provide different packet processing policies on the OLT. Select one of them based on site requirements. For details, see the **pitp** command.
   - The port level: In global config mode, run the **pitp port** or **pitp board** command to enable PITP at the port level.
   - The VLAN level:
     a. In global config mode, run the **vlan service-profile** command to create a VLAN service profile.
     b. Run the **pitp enable** command to enable PITP at the VLAN level.
     c. Run the **commit** command to make the profile configuration take effect.
     d. Run the **quit** command to quit the VLAN service profile mode.
     e. Run the **vlan bind service-profile** command to bind the created VLAN service profile to a VLAN.
   - The service port level: In global config mode, run the **pitp service-port** command to enable PITP at the service port level.
2. On the OLT, run the **pitp permit-forwarding service-port** command with the **enable** parameter selected, to allow ONU PPPoE packets to carry a vendor tag.

----End

Copyright © Huawei Technologies Co., Ltd.

12.4.1.12 Verifying Services

In the FTTO scenario, ONUs are installed at users' houses or in business buildings which are far away from the central equipment room. ONUs provide remote service verification methods including PPPoE dialup emulation, call emulation, and multicast emulation to facilitate configuration and commissioning engineers to verify services remotely after service configuration.

Prerequisites

ONUs and upper-layer devices have been connected properly. The BRAS and MGC/IMS have been configured.

Background

Remote Service Verification Method	Function	Description
PPPoE dialup emulation	An ONU simulates a PPPoE user terminal software to perform dialup and interact with the BRAS to verify the connectivity between the ONU and BRAS.	● PPPoE dialup emulation requires a service flow which does not belong to a QinQ VLAN. ● A user name, password, and authentication mode must be configured on the BRAS for the PPPoE dialup emulation. ● An ONU supports a maximum of a PPPoE dialup emulation.
Call Emulation	An ONU simulates a voice user to make a call to check whether the voice service data is correctly configured. You can also use the call emulation function to locate a fault when the voice service is faulty.	● An ONU can simulate a caller or callee to communicate with a phone in a call. In this case, only a functional phone is required in the central office where the acceptance personnel locate. ● An ONU supports only once call emulation.
Multicast emulation	This function enables you to simulate a multicast user going online and lead the program stream to an ONU. You can check whether the multicast service is normal by checking the real-time traffic of the multicast program.	Multicast services configured in the dynamic controllable multicast mode do not support this function.

Copyright © Huawei Technologies Co., Ltd.

Data plan

Item	Data	Remarks
PPPoE dialup emulation parameters	PPPoE user name: test@huawei Password: test	The user name, password, and authentication mode for the emulation test must be configured on the BRAS. The entered user name, password, and authentication mode must be consistent with those configured on the BRAS.
Call emulation parameters	ONU POTS ID: 1	The default values are used. You can run the **display pots emulational configuration** command to check the parameter values.
Multicast emulation parameters	Multicast service flow ID: 1 MVLAN: 1000 IP address of the multicast program: 224.1.1.10	-

Procedure

- Verify the Internet access service using PPPoE dialup emulation.
  1. In the xPON board mode, run the **pppoe simulate start** command to start a PPPoE dialup emulation test.

     The service is functional if the test result is **success**. The following test uses GPON as an example:

```
huawei(config)#interface gpon 0/1
huawei(config-if-gpon-0/1)#pppoe simulate start
{ portid<U><0,7> }:0
{ ontid<U><0,127> }:1
{ eth<K>|untagged<K>|vlanid<U><0,4095> }:eth
{ ont-portid<U><1,8> }:4
{ untagged<K>|vlanid<U><0,4095> }:100
{ priority<U><0,7>|user-name<K> }:user-name
{ username<S><Length 1-64> }:test@huawei
{ user-password<K> }:user-password
{ password<S><Length 1-64> }:test
{ authentication-mode<K> }:authentication-mode
{ protocol<E><chap,pap> }:chap

  Command:
          pppoe simulate start 0 1 eth 4 100 user-name test@huawei user-
password
 test authentication-mode chap

huawei(config-if-gpon-0/1)#
  ---------------------------------
  ONT PPPoE Test Result
  ---------------------------------
  F/S/P                : 0/1/0
  ONT-ID               : 1
  ONT ETH Port ID      : 4
  ONT Vlan ID          : 100
  Vlan Priority        : -
  Emluator result      : Success
```


Copyright © Huawei Technologies Co., Ltd.

```
  Session ID           : 18814
  User IP              : 172.16.100.109
  Gateway IP           : 172.16.100.1
  ---------------------------------
```

- Troubleshooting methods for the Internet access service
  1. Check whether configurations are complete on the OLT.
     - Run the **display ont info** command to query the ONU status to check whether the ONU is registered successfully.
     - Run the **display service-port** command to check whether the Internet access service flow is configured and whether the inner VLAN ID of the service flow is consistent with that in the data plan.
     - If a native VLAN is configured for the Ethernet port on the ONU, run the **display ont port attribute** command in the xPON board mode to check whether the native VLAN is correct.
  2. Check the upstream and downstream ports by checking the MAC address learning status.
     a. Run the **display mac-address vlan** command to check the MAC address learning status of the Internet service VLAN.
        - If the upstream port does not learn a MAC address, check the network connections between the upstream port and upper-layer devices and check the configurations of upper-layer devices.
        - If the downstream port does not learn a MAC address, check whether the ONU is activated, whether the PC is connected to the right port on the ONU, and whether the PC is working properly.
     b. Run the **display ont-learned-mac** command to check whether the ONU connecting to the PON port learned any MAC addresses.

        If not, check whether the ONU properly connects to the PC or home gateway (HGW).
- Verify the voice service using call emulation.
  1. Run the **ont emulational call** command to configure a call emulation test.

```
huawei(config)#test
huawei(config-test)#ont emulational call caller-port 0/1/0 1 1 telno
28777192
{ <cr>|caller-stop-time<K> }:

  Command:
          ont emulational call caller-port 0/1/0 1 1 telno 28777192
```

  2. The ONU outputs the call emulation result after the test is complete.

     The service is functional if the test result is **success**.

```
huawei(config-test)#
  ------------------------------------------------------------------
  F/S/P                : 0/1/0
  ONT-ID               : 0
  ONT-POTSID           : 1
  Test type            : caller emulational call test
  Detected number      : 28777192
  Reported number      : 28777192
  Current status       : test end
  Test Result          : success
  ------------------------------------------------------------------
```

- Troubleshooting methods for the voice service.

Copyright © Huawei Technologies Co., Ltd.

1. Check whether configurations are complete on the OLT.
   - Run the **display ont info** command to query the ONU status to check whether the ONU is registered successfully.
   - Run the **display service-port** command to check whether the voice service flow is configured and whether the inner VLAN ID of the service flow is consistent with that in the data plan.
2. Check the upstream and downstream ports by checking the MAC address learning status.

   Run the **display mac-address vlan** command to check the MAC address learning status of the voice service VLAN.
   - If the upstream port does not learn a MAC address, check the network connections between the upstream port and upper-layer devices and check the configurations of upper-layer devices.
   - If the downstream port does not learn a MAC address, check whether the ONU is activated and whether physical links are normal.
   - If both the upstream and downstream ports can learn the MAC address, record the MAC address of the ONU and log in to the service router (SR) to check whether an IP address is allocated to the MAC address.
3. Check the registration status of the voice service.
   - You can run the **display ont port state** command on the OLT to query the call connection status on the POTS port. If **Call State** is **RegisterFail** or **Connecting** for a long time, check whether the voice configuration on the MGC/SIP server is consistent with that on the ONU.
   - If the ONU uses the H.248 protocol, you can run the **display ont mg status** command on the OLT to query the registration status of the MG interface that connects to the ONU. If **MG Status** is **UnRegistered** or **Registering** for a long time, check whether the voice configuration on the MGC/SIP server is consistent with that on the ONU.
   - You can query the registration status of the voice service on the ONU web page. If the query result shows that the registration fails or the voice service is in the registering state for a long time, check whether the voice configuration on the MGC/SIP server is consistent with that on the ONU.

- Verify the multicast service using multicast emulation.
  1. Run the **igmp static-join** command to simulate a multicast user to order a multicast program.

     ```
     huawei(config)#btv
     huawei(config-btv)#igmp static-join service-port 1 ip 224.1.1.10 vlan 1000
     ```

     NOTE

     If the multicast program is obtained dynamically, **igmp static-join** can be executed successfully only when the range for obtaining the dynamic program is set.
  2. Run the **display igmp user** command to query the status of the multicast user.

     The multicast user is normal if the queried result is **online**.

     ```
     huawei(config-btv)#display igmp user service-port 1
       User                        : 0/1/0/1
       State                       : online
       Authentication              : no-auth
       Quick leave                 : MAC-based
       IGMP flow ID                : 1
     ```


Copyright © Huawei Technologies Co., Ltd.

```
  Video flow ID              : 1
  Log switch                 : enable
  Bind profiles              : -
  IGMP version               : IGMP v3
  Current version            : IGMP v3
  Current IGMP IPv6 version  : IGMP IPv6 v2
  Available programs         : 8
  Global leave               : disable
  User max bandwidth         : no-limit
  Used bandwidth(kbps)       : 0
  Used bandwidth
  to max bandwidth(%)        : -
  Total video bandwidth      : -
  Mcast video bandwidth      : -
  Active program list

--------------------------------------------------------------------------
--
  Program name     VLAN  IP/MAC           State           Start time

--------------------------------------------------------------------------
--
  PROGRAM-5        1000  224.1.1.10       watching        2011-10-29
                                                         16:33:41+08:00

--------------------------------------------------------------------------
--
  Total: 1
```

3. Run the **display multicast flow-statistic** command to query the real-time traffic of the multicast program.

   The multicast program can be ordered if the queried result is a non-empty value.

```
huawei(config-btv)#display multicast flow-statistic vlan 1000 ip
224.1.1.10
{ <cr>|sourceip<K> }:

  Command:
          display multicast flow-statistic vlan 1000 ip 224.1.1.10
  Command is being executed. Please wait...
  Multicast flow statistic result: 8736(kbps)
```

----End

12.4.2 Gateway Networking

This section describes the configurations for the Internet access, voice, and video services on optical network units (ONUs) in gateway networking.

12.4.2.1 Service Requirements and Usage Scenario

Small- and medium-sized enterprise (SME) is positioned for small- and medium-sized enterprises with branches, campuses, and net bars.

Service Requirements

In the SME scenario, optical network units (ONUs) work in gateway mode.

- Users connect to an ONU through an enterprise LAN switch. As a Dynamic Host Configuration Protocol (DHCP) client, the ONU obtains a public IP address through PPPoE dialup. As a DHCP server, the ONU assigns private IP addresses to the users. After Network Address Translation (NAT), all the users connected to the LAN switch use a public IP

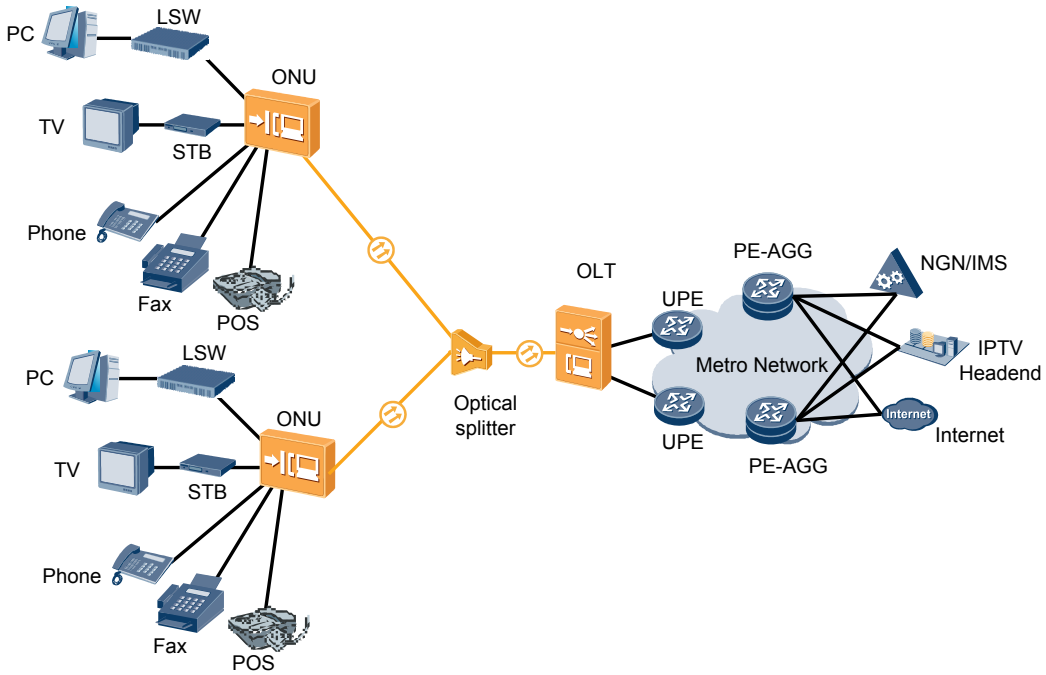
Copyright © Huawei Technologies Co., Ltd.

address to access the Internet. The ONU connects to the optical line terminal (OLT) in GPON access mode and then connects to the upper-layer network, to provide the high-speed Internet access service.

- Voice service ports connect to phone sets, fax machines, or point of sale (POS) machines.
- TVs connect to an ONU through set top boxes (STBs) to receive VoD and multicast services.
- The Internet access, voice, and IPTV services are secure.
  - The Internet access service is protected against unauthorized access, user account forgery or unauthorized borrowing, MAC or IP address spoofing, and attacks from malicious users.
  - The voice and IPTV services are protected against MAC or IP address spoofing, attacks from malicious users, and heavy traffic.
- A service fault is easy to locate, and services are easy to maintain.

Usage Scenario

Figure 12-9 Gateway networking

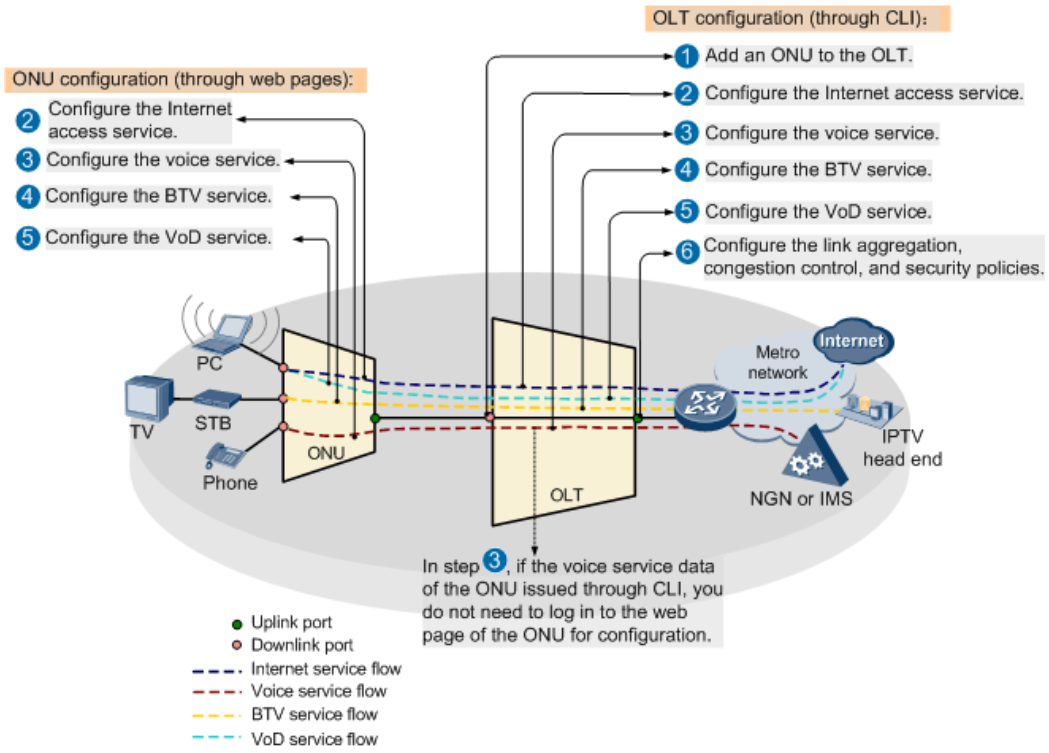


12.4.2.2 Configuration Procedure

Figure 12-10 shows the configuration procedure in the FTTO small- and medium-sized enterprises (SME) scenario.

Copyright © Huawei Technologies Co., Ltd.

Figure 12-10 Configuration procedure in the FTTO SME scenario



The following table lists the detailed description steps.

Item	Procedure		Remarks
OLT	**Adding an ONU to an OLT**		Services can be configured for an ONU only after the ONU is successfully added to an OLT.
OLT ONU	**Configuring the Internet Access Service**		-
OLT ONU	Configuring the Voice Service	**Configuring the H.248-based Voice Service (on a Web Page)**	**NOTE** The H.248 and SIP protocols are mutually exclusive for the VoIP service. Only one of them is configured at a time.
		Configuring the H.248-based Voice Service (Through the CLI)	

Copyright © Huawei Technologies Co., Ltd.

Item	Procedure		Remarks
		Configuring the SIP-based Voice Service (on a Web Page)	
		Configuring the SIP-based Voice Service (Through the CLI)	
OLT	Configuring the BTV Service		IPTV services include the VoD and multicast services that are different in configuration procedures and need to be configured separately.
OLT			
OLT	Configuring Link Aggregation, Congestion Control, and Security Policy		Service reliability is improved by configuring uplink aggregation and priority scheduling policy for queues in global configuration mode, and service security is improved by configuring security policy in global configuration mode.
OLT	Verifying Services		The OLT provides remote verification methods including ONU PPPoE and DHCP dialup emulation and call emulation for configuration and commissioning engineers to verify services remotely after service configuration, avoiding a second on-site operation.

12.4.2.3 Adding an ONU to an OLT

Services can be configured for an ONU only after the ONU is successfully added to an OLT.

Data Plan

Table 12-34 Data plan

Item	Data
DBA profile	Profile name: ftto_dba Profile type: type3 Assured bandwidth: 8 Mbit/s Maximum bandwidth: 50 Mbit/s

Copyright © Huawei Technologies Co., Ltd.

Item	Data
ONU line profile	Profile name: ftto_line T-CONT ID: 4 GEM port ID for management services: 11 GEM port ID for voice services: 12 GEM port ID for video services: 13 GEM port ID for Internet access services: 14
ONU service profile	Profile name: ftto_ser ONU port capability set: adaptive
Network topology data	PON port: 0/1/0 ONU IDs: 1 and 2

Procedure

Step 1 Configure GPON ONU profiles.

GPON ONU profiles include the DBA profile, line profile, service profile, and alarm profile.

- DBA profile: A DBA profile describes GPON traffic parameters. A T-CONT is bound to a DBA profile for dynamic bandwidth allocation, improving upstream bandwidth utilization.
- Line profile: A line profile describes the binding between the T-CONT and the DBA profile, the QoS mode of the traffic stream, and the mapping between the GEM port and the ONU-side service.
- Service profile: A service profile provides the service configuration channel for the ONU that is managed by using optical network terminal management and control interface (OMCI).
- Alarm profile: An alarm profile contains a series of alarm thresholds to measure and monitor the performance of activated ONU lines. When a statistical value reaches the threshold, the host is notified and an alarm is reported to the log host and the NMS.

1. Configure a DBA profile.

   Run the **display dba-profile** command to query existing DBA profiles in the system. If the existing DBA profiles in the system do not meet the requirements, run the **dba-profile add** command to add a DBA profile.

   Create the same DBA profile for different types of services. Set the profile name to **ftto_dba**, profile type to **type3**, assured bandwidth to 8 Mbit/s, and maximum bandwidth to 50 Mbit/s.

   ```
   huawei(config)#dba-profile add profile-name ftto_dba type3 assure 8192 max 51200
   ```

   NOTE

   The DBA implementation is based on an ONU. Therefore, select a DBA profile of the proper bandwidth type and configure proper bandwidth according to the service types and total user count of the ONU. Note that the sum of the fixed bandwidth and the assured bandwidth must not be greater than the total bandwidth of the PON port.

Copyright © Huawei Technologies Co., Ltd.

2. Configure an ONU line profile.

   Create a GPON ONU line profile, named **ftto_line**, and bind it to the DBA profile **ftto_dba**.

   ```
   huawei(config)#ont-lineprofile gpon profile-name ftto_line
   huawei(config-gpon-lineprofile-1)#tcont 4 dba-profile-name ftto_dba
   ```

   Create different GEM ports according to different service types, in which

   - GEM port 11 is used to carry management services.
   - GEM port 12 is used to carry voice services.
   - GEM port 13 is used to carry video services.
   - GEM port 14 is used to carry Internet access services.

   ```
   huawei(config-gpon-lineprofile-1)#gem add 11 eth tcont 4
   huawei(config-gpon-lineprofile-1)#gem add 12 eth tcont 4
   huawei(config-gpon-lineprofile-1)#gem add 13 eth tcont 4
   huawei(config-gpon-lineprofile-1)#gem add 14 eth tcont 4
   ```

   NOTE

   1. To change the default QoS mode, run the **qos-mode** command to set the QoS mode to **gem-car** or **flow-car**, and run the **gem add** command to set the index of the traffic profile bound to the GEM port.
   2. When the QoS mode is priority-queue (PQ), the default queue priority is 0; when the QoS mode is flow-car or gem-car, traffic profile 6 is bound to the GEM port by default (no rate limitation).

   After the configurations are complete, run the **commit** command to apply the parameters settings.

   ```
   huawei(config-gpon-lineprofile-1)#commit
   huawei(config-gpon-lineprofile-1)#quit
   ```

3. Configure an ONU service profile.

   Create a GPON ONU service profile, named **ftto_ser**. Configure the capability set of the ETH port and POTS port to **adaptive**. Then the system automatically adapts to the ONU according to the actual capability of the online ONU.

   ```
   huawei(config)#ont-srvprofile gpon profile-name ftto_ser
   huawei(config-gpon-srvprofile-1)#ont-port eth adaptive pots adaptive
   ```

   After the configurations are complete, run the **commit** command to apply the parameters setting.

   ```
   huawei(config-gpon-srvprofile-1)#commit
   huawei(config-gpon-srvprofile-1)#quit
   ```

4. (Optional) Add an alarm profile.

   - The default GPON alarm profile 1 is used. The alarm thresholds of the default alarm profile are 0, which indicates that no alarm is generated.
   - In this example, the default alarm profile is used, and therefore the configuration of the alarm profile is not required.
   - Run the **gpon alarm-profile add** command to configure a GPON alarm profile, which is used for monitoring the performance of an activated ONU line.

Step 2 Add an ONU.

Connect two ONUs to GPON port 0/1/0. Set the ONU IDs to **1** and **2**, SNs to **32303131D659FD40** and **6877687714852901**, passwords to **0100000001** and **0100000002**, discovery mode for password authentication to **once-on**, and management mode to **OMCI**. Bind the two ONUs to ONU line profile **ftto_line** and ONU service profile **ftto_ser**.

There are two methods of adding an ONU: add an ONU offline and confirm an automatically discovered ONU.

Copyright © Huawei Technologies Co., Ltd.

- Add ONUs offline.

  If the password of an ONU is known, run the **ont add** command to add an ONU offline.

```
huawei(config)#interface gpon 0/1
huawei(config-if-gpon-0/1)#ont add 0 1 password-auth 0100000001 once-on no-aging
omci ont-lineprofile-name
 ftto_line ont-srvprofile-name ftto_ser
huawei(config-if-gpon-0/1)#ont add 0 2 password-auth 0100000002 once-on no-aging
omci ont-lineprofile-name
 ftto_line ont-srvprofile-name ftto_ser
```

- Confirm automatically discovered ONUs

  If the password or SN of an ONU is unknown, run the **port** ***portid*** **ont-auto-find** command in GPON mode to enable the ONU auto-discovery function of the GPON port. Then, run the **ont confirm** command to confirm the ONU.

```
huawei(config)#interface gpon 0/1
huawei(config-if-gpon-0/1)#port 0 ont-auto-find enable
huawei(config-if-gpon-0/1)#display ont autofind 0
  //After this command is executed, the information about all ONUs connected to
the GPON port through optical splitters is displayed.

huawei(config-if-gpon-0/1)#ont confirm 0 ontid 1 sn-auth 32303131D659FD40 omci
ont-lineprofile-name
 ftto_line ont-srvprofile-name ftto_ser
huawei(config-if-gpon-0/1)#ont confirm 0 ontid 2 sn-auth 6877687714852901 omci
ont-lineprofile-name
 ftto_line ont-srvprofile-name ftto_ser
```

  NOTE

  If multiple ONUs of the same type bound to the same line profile or service profile are connected to the same port, you can bulk add ONUs by bulk confirming automatically discovered ONUs to make configuration easier and more efficient. To do so, the preceding command can be modified as follows:

```
huawei(config-if-gpon-0/1)#ont confirm 0 all sn-auth omci ont-lineprofile-name
ftto_line
ont-srvprofile-name ftto_ser
```

- (Optional) Bind the alarm profile to the ONU.

  The default profile 1 is used in this example.

```
huawei(config-if-gpon-0/1)#ont alarm-profile 0 1 profile-id 1
huawei(config-if-gpon-0/1)#ont alarm-profile 0 2 profile-id 1
```

Step 3 Check ONU status.

After an ONU is added, run the **display ont info** command to query the current status of the ONU. Ensure that **Config flag** of the ONU is **active**, **Run State** is **online**, **Config state** is **normal**, and **Match state** is **match**.

```
huawei(config-if-gpon-0/1)#display ont info 0 1
  ------------------------------------------------------------------------
  F/S/P                : 0/1/0
  ONT-ID               : 1
  Control flag         : active    //Indicates that the ONU is
activated.
  Run state            : online    //Indicates that the ONU goes online
successfully.
  Config state         : normal    //Indicates that the configuration state of the
ONU is normal.
  Match state          : match     //Indicates that the capability profile bound to
the ONU is consistent with the actual capability of the ONU.
...//The rest of the response information is omitted.
```

When **Config state** is **failed**, **Run state** is **offline**, or **Match state** is **mismatch**:

- If **Control flag** is **deactive**, run the **ont active** command in GPON mode to activate the ONU.

Copyright © Huawei Technologies Co., Ltd.

- If **Run state** is **offline**, a physical line may be broken or the optical module may be damaged. Check the line and the optical module.
- If **Config state** is **failed**, the configured ONU capability exceeds the actual ONU capability. In this case, run the **display ont failed-configuration** command in the diagnose mode to check the failed configuration item and the failure cause. Then, rectify the fault accordingly.
- If the ONU does not match, that is, **Match state** is **mismatch**, the port types and number of ports undermatch the actual port types and number of ports supported by the ONU. In this case, run the **display ont capability** command to query the actual capability of the ONU, and then select one of the following modes to modify the ONU configuration:
  - Create a proper ONU profile according to the actual capability of the ONU, and then run the **ont modify** command to modify the configuration data of the ONU.
  - Modify the ONU profile according to the actual capability of the ONU and save the modification. Then, the ONU automatically recovers the configuration successfully.

----End

12.4.2.4 Configuring the Internet Access Service

The OLT is connected to the remote ONU through a GPON port to provide users with high-speed Internet access services.

Prerequisite

- The OLT is connected to the BRAS.
- Related configurations are performed on the BRAS according to the authentication and accounting requirements for dialup users. For details about the configuration, see the configuration guide.
- The ONU has been added to the OLT. For details, see **12.3.3 Adding an ONU to an OLT**.

Data Plan

Table 12-35 Data plan

Item	Data
ONU line profile	Profile name: ftto_line T-CONT ID: 4 GEM port ID for Internet access service: 14
ONU service profile	Profile name: ftto_ser ONU port capability set: adaptive

Procedure

- Configure the OLT.
  1. Configure a traffic profile.

Copyright © Huawei Technologies Co., Ltd.

Run the **display traffic table ip** command to query existing traffic profiles in the system. If the traffic profiles existing in the system do not meet the requirements, you need to run the **traffic table ip** command to add a traffic profile.

Set the profile ID to ftto_hsi, the CIR to 4 Mbit/s, and the priority to 0. In addition, configure the scheduling mode so that packets are scheduled according to their priorities.

```
huawei(config)#traffic table ip name ftto_hsi cir 4096 priority 0 priority-
policy local-setting
```

2. Configure the mapping between a GEM port and a VLAN. Create a service VLAN and a service flow.

Table 12-36 Scenario plan

Scenario	VLAN Plan	VLAN Translation Policy
gateway ONU	Double-tagged VLAN ● S-VLAN ID: 100 ● S-VLAN type: smart ● S-VLAN attribute: stacking ● C-VLAN ID: 1001 ● C'-VLAN ID: 1010-1011	ONU: Configure a VLAN for all ONUs and add the same C-VLAN tag to packets. All ONUs are in the same C-VLAN. OLT: The OLT switches between the C-VLAN tag and the S-VLAN +C'-VLAN tag. All ONUs are in different C-VLANs.

Configure the mapping between a GEM port and a VLAN. The service flow of user VLAN 1001 is mapped to GEM port 14 in the ONU line profile.

```
huawei(config)#ont-lineprofile gpon profile-name ftto_line
huawei(config-gpon-lineprofile-1)#gem mapping 14 0 vlan 1001
huawei(config-gpon-lineprofile-1)#commit
huawei(config-gpon-lineprofile-1)#quit
```

Create a service VLAN and add an upstream port to it. Add upstream port 0/19/0 to VLAN 100.

```
huawei(config)#vlan 100 smart
huawei(config)#vlan attrib 100 stacking
huawei(config)#port vlan 100 0/19 0
```

Create service flows. Set the service VLAN to 100, GEM port ID to 14, and user VLAN to 1001, and use traffic profile ftto_hsi.

```
huawei(config)#service-port vlan 100 gpon 0/1/0 ont 1 gemport 14 multi-
service
user-vlan 1001 tag-transform translate-and-add inner-vlan 1010 inbound
traffic-table name
ftto_hsi outbound traffic-table name ftto_hsi
huawei(config)#service-port vlan 100 gpon 0/1/0 ont 2 gemport 14 multi-
```


Copyright © Huawei Technologies Co., Ltd.

```
service
user-vlan 1001 tag-transform translate-and-add inner-vlan 1011 inbound
traffic-table name
ftto_hsi outbound traffic-table name ftto_hsi
```

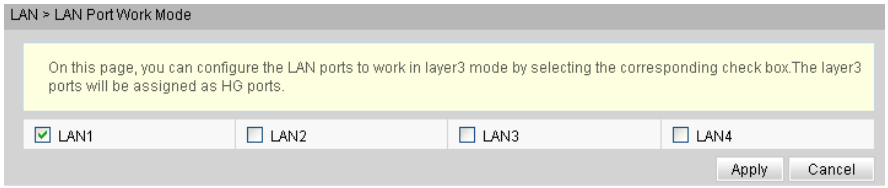
3. Save the data.

```
huawei(config)#save
```

- Configure an optical network terminal (ONU) on the Web page.

  Layer 3 route mode is used for connecting an ONU to the upper-layer device. IP addresses of users' PCs are allocated by the DHCP IP address pool on the ONU. PPPoE auto dialup is performed on the ONU. Parameters of the WAN port must be configured on the ONU.

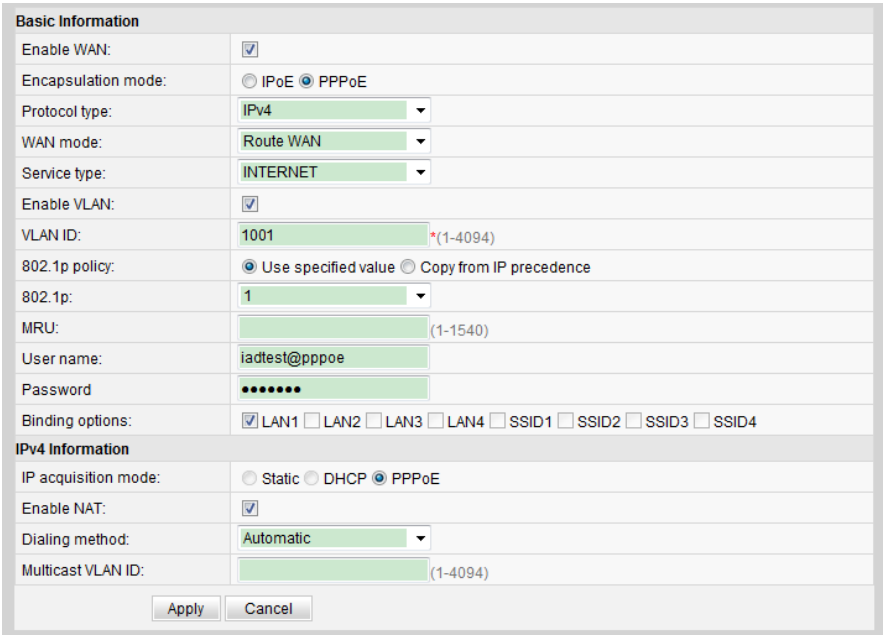
  1. Log in to the Web configuration window.
     a. Configure the IP address of the PC network adapter to be in the same network segment as the IP address of the local maintenance Ethernet port on the ONU (default: **192.168.100.1**).
     b. Open the Web browser, and enter the IP address of the local maintenance Ethernet port of the ONU.
     c. On the login window, enter the user name (default: **telecomadmin**) and password (default: **admintelecom**) of the administrator. After the password authentication is passed, the Web configuration interface is displayed.
  2. Configure the working mode of a LAN port.
     a. In the navigation tree, choose **LAN** > **LAN Port Work Mode**. Select the check box of LAN 1 and set LAN1 to work in the Layer 3 mode.



     b. Click **Apply** to apply the configuration.
  3. Configure parameters of a WAN port.
     a. In the navigation tree, choose **WAN** > **WAN Configuration**.
     b. In the right pane, click **New**. In the dialog box that is displayed, configure parameters of a WAN port as follows:
        - WAN Connection: Enable
        - Encapsulation Mode: PPPoE
        - WAN mode: Route WAN
        - Service type: INTERNET (For configuring the Internet access service, **INTERNET** or a combination containing **INTERNET** needs to be selected.)
        - VLAN ID: 1001 (The VLAN ID of the ONU must be the same as the user-side VLAN ID configured on the OLT.)
        - 802.1p: 1
        - User Name: iadtest@pppoe, Password: iadtest (The user name and password must be the same as the user name and password configured on the BRAS.)
        - Binding options: LAN1
        - IP acquisition Mode: PPPoE

Copyright © Huawei Technologies Co., Ltd.

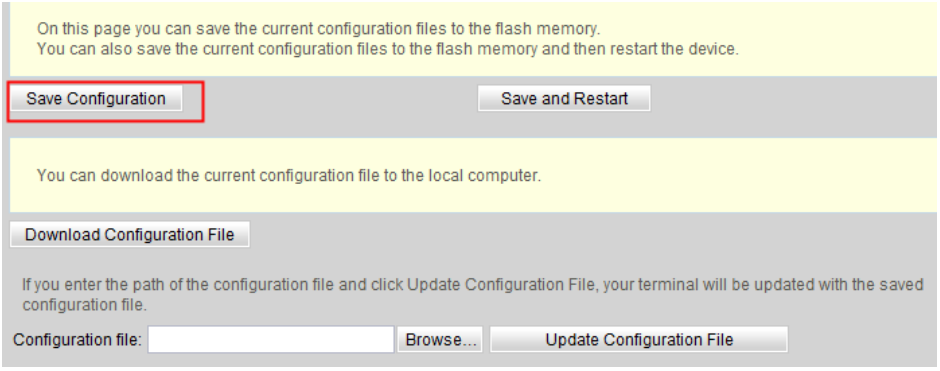
- NAT: Enable (NAT must be enabled to configure the Internet access service.)



c. Click **Apply** to apply the configuration.

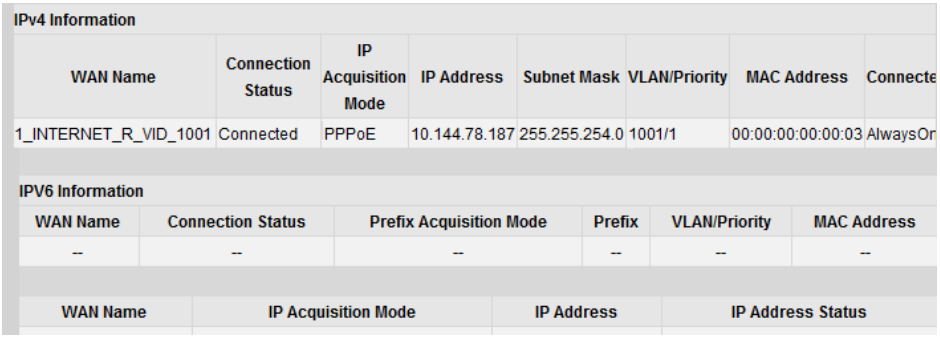
4. Save the configuration.

   In the navigation tree, choose **System Tools** > **Configuration File**. In the right pane, click **Save Configuration** to save the configuration.



5. Check the ONU connection status.

   In the navigation tree, choose **Status** > **WAN Information**. In the right pane, **Status** is **Connected** and the obtained IP address is displayed at **IP Address**.



----End

Copyright © Huawei Technologies Co., Ltd.

12.4.2.5 Configuring the H.248-based Voice Service (on a Web Page)

The OLT is connected to the remote ONU through a GPON port to provide users with the IP-based high-quality and low-cost VoIP service.

Prerequisite

- The interface data and POTS port data corresponding to the MG interface have been configured on the MGC.
- The OLT has been connected to the MGC. The OLT can ping the IP address of the MGC server successfully.
- The ONU has been added to the OLT. For details, see **12.3.3 Adding an ONU to an OLT**.
- Different voice services require different ONU software versions. Before the configuration, ensure that the ONU software version supports H.248. For details, see relevant ONU manuals.

Context

Table 12-37 Data plan

Item	Data
ONU line profile	Profile name: ftto_line T-CONT ID: 4 GEM port ID: 12
ONU service profile	Profile name: ftto_ser ONU port capability set: adaptive
Networking data	IP address of the MGC server: 200.200.200.200/24 Port ID of the MGC server: 2944

Procedure

- Configure the OLT.
  1. Configure a traffic profile.

     Set the profile name to **ftto_voip** and do not limit the upstream and downstream rates. Set the priority to **5** and packets are scheduled according to the priority carried.

     Run the **display traffic table ip** command to query existing traffic profiles in the system. If the existing traffic profiles in the system do not meet the requirements, run the **traffic table ip** command to add a traffic profile.

     ```
     huawei(config)#traffic table ip name ftto_voip cir off priority 5 priority-policy
      local-setting
     ```

  2. Configure the mapping between a GEM port and a VLAN. Create a service VLAN and a service flow.

Copyright © Huawei Technologies Co., Ltd.

Table 12-38 Scenario plan

Scenario	VLAN Plan	VLAN Translation Policy
Scenario 1	Single VLAN tag ● S-VLAN ID: 300 ● S-VLAN type: smart ● S-VLAN attribute: common ● C-VLAN ID: 300	ONU: Configure a VLAN for all ONUs and add the same C-VLAN tag to packets. All ONUs are in the same C-VLAN. OLT: The OLT transparently transmits VLAN tags (the C-VLAN is the same as the planned S-VLAN).
Scenario 2	Single VLAN tag ● S-VLAN ID: 300 ● S-VLAN type: smart ● S-VLAN attribute: common ● C-VLAN ID: 3001	ONU: Configure a VLAN for all ONUs and add the same C-VLAN tag to packets. All ONUs are in the same C-VLAN. OLT: The OLT switches between C-VLAN tags and S-VLAN tags (C-VLAN is different from the planned S-VLAN).

Scenario 1:

Configure the mapping between a GEM port and a VLAN. The service flow of user VLAN 300 is mapped to GEM port 12 in the ONU line profile.

```
huawei(config)#ont-lineprofile gpon profile-name ftto_line
huawei(config-gpon-lineprofile-1)#gem mapping 12 2 vlan 300
huawei(config-gpon-lineprofile-1)#commit
huawei(config-gpon-lineprofile-1)#quit
```

Create a service VLAN and add an upstream port to it. Add upstream port 0/19/0 to VLAN 300.

```
huawei(config)#vlan 300 smart
huawei(config)#port vlan 300 0/19 0
```

Create service flows. Set the service VLAN to 300, GEM port ID to 12, and user VLAN to 300, and use traffic profile **ftto_voip**.

```
huawei(config)#service-port vlan 300 gpon 0/1/0 ont 1 gemport 12 multi-
service
 user-vlan 300 inbound traffic-table name ftto_voip outbound traffic-table
name
ftto_voip
huawei(config)#service-port vlan 300 gpon 0/1/0 ont 2 gemport 12 multi-
service
 user-vlan 300 inbound traffic-table name ftto_voip outbound traffic-table
name
ftto_voip
```

Scenario 2:

Copyright © Huawei Technologies Co., Ltd.

Configure the mapping between a GEM port and a VLAN. The service flow of user VLAN 3001 is mapped to GEM port 12 in the ONU line profile.

```
huawei(config)#ont-lineprofile gpon profile-name ftto_line
huawei(config-gpon-lineprofile-1)#gem mapping 12 2 vlan 3001
huawei(config-gpon-lineprofile-1)#commit
huawei(config-gpon-lineprofile-1)#quit
```

Create a service VLAN and add an upstream port to it. Add upstream port 0/19/0 to VLAN 300.

```
huawei(config)#vlan 300 smart
huawei(config)#vlan attrib 300 stacking
huawei(config)#port vlan 300 0/19 0
```

Create service flows. Set the service VLAN to 300, GEM port ID to 12, and user VLAN to 3001. Use traffic profile **ftto_voip**.

```
huawei(config)#service-port vlan 300 gpon 0/1/0 ont 1 gemport 12 multi-
service
user-vlan 3001 tag-transform translate inbound traffic-table name
ftto_voip outboun
d traffic-table name ftto_voip
huawei(config)#service-port vlan 300 gpon 0/1/0 ont 2 gemport 12 multi-
service
user-vlan 3001 tag-transform translate inbound traffic-table name
ftto_voip outboun
d traffic-table name ftto_voip
```

3. Enable the ARP proxy function.

   Voice media streams for different users of the same S-VLAN fail to interchange because the service ports of the smart VLAN are isolated from each other. Therefore, the ARP proxy function needs to be enabled on the OLT.

   ```
   huawei(config)#arp proxy enable
   huawei(config)#interface vlanif 300
   huawei(config-if-vlanif300)#arp proxy enable
   huawei(config-if-vlanif300)#quit
   ```

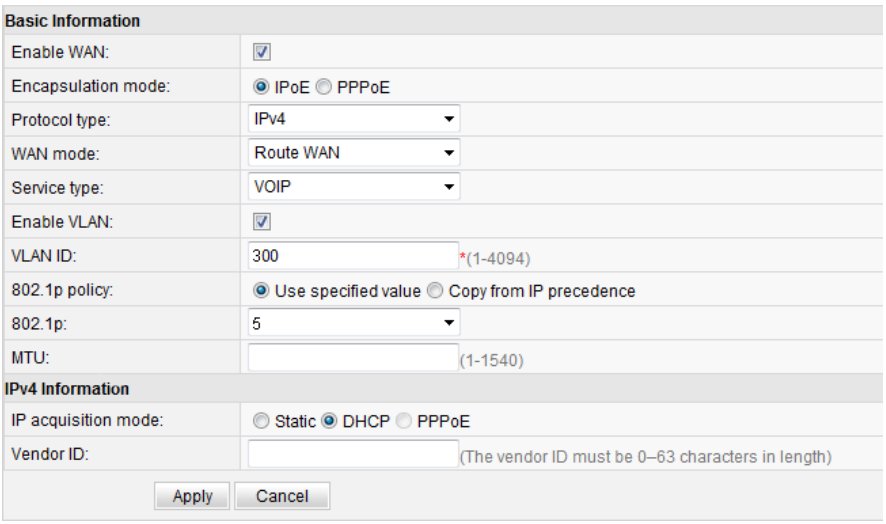
4. Save the data.

   ```
   huawei(config)#save
   ```

- Configure the ONU on the Web page.
  1. Log in to the Web configuration window.
     a. Configure the IP address of the PC network adapter to be in the same network segment as the IP address of the local maintenance Ethernet port on the ONU (default: **192.168.100.1**).
     b. Open the Web browser, and enter the IP address of the local maintenance Ethernet port of the ONU.
     c. On the login window, enter the user name (default: **telecomadmin**) and password (default: **admintelecom**) of the administrator. After the password authentication is passed, the Web configuration interface is displayed.
  2. Configure parameters of a voice WAN port.
     a. In the navigation tree, choose **WAN** > **WAN Configuration**.
     b. In the right pane, click **New**. In the dialog box that is displayed, configure parameters of a WAN port as follows:
        - WAN Connection: Enable

Copyright © Huawei Technologies Co., Ltd.

- Service List: VoIP (For configuring the VoIP service, VoIP or a combination containing VoIP needs to be selected.)
- Mode: Route
- VLAN ID: 300 (The VLAN ID of the ONU must be the same as the user-side VLAN ID configured on the OLT.)
- 802.1p: 5
- IP Acquisition Mode: DHCP



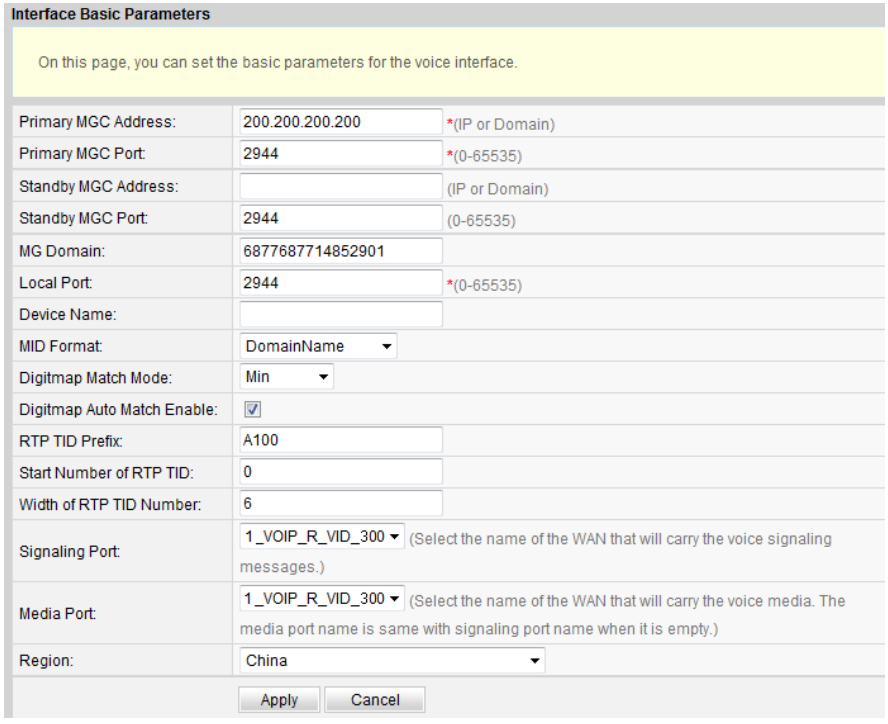
c. Click **Apply** to apply the configuration.

3. Configure the parameters of the H.248-based voice interface.
   a. In the navigation tree, choose **Voice** > **VoIP Basic Configuration**.
   b. In the right pane, configure the parameters of the H.248-based voice interface as follows (other parameters use the default settings):
      - Set **MGC Address** below **Primary Server** to **200.200.200.200**.
      - MID Format: DomainName
      - MG Domain: 6877687714852901
      - Signaling Port: 1_VOIP_R_VID_300
      - Region: China

Copyright © Huawei Technologies Co., Ltd.

NOTE

- The parameters of the H.248-based voice interface must be consistent with the corresponding configuration on the media gateway controller (MGC).
- If dual-homing is configured, **MGC Address** below **Secondary Server** must be configured.
- **MID Format** can be set to **Domain Name**, **IP**, or **Device**. If **MID Format** is set to **Domain Name** or **Device**, the setting must be consistent with the corresponding configuration on the MGC.
- **Domain Name** is ONU's domain name registered with the MGC. It is globally unique. **Domain Name** in this example is ONU's SN.
- If **Media Port** is empty, the parameter value is the same as **Signaling Port**. The media streams are not isolated from signaling streams. If the upper-layer network requires isolation of media streams from signaling streams, create different traffic streams for the media streams and signaling streams on the OLT, create different WAN ports on the ONU, and bind the created WAN ports to **Media Port** and **Signaling Port**.
- **Profile Index** can be set to **Default**, **BT**, **FT**, **KPN**, **PCCW**, **ZTE**, or **BELL**. Choose the value based on the MGC type. **Profile Index** is set to **Default** (indicating interconnection with Huawei MGC) in this example. If the settings do not meet requirements, configure **UserDefine**. For details about how to configure this parameter, contact Huawei technical support engineers.
- When the ONU is interconnected with a third-party softswitch, check **RTP TID Prefix**, **Start Number of RTP TID**, and **Width of RTP TID Number**.



c. Click **Apply** to apply the configuration.

4. Configure parameters of the H.248-based voice users.

a. In the navigation tree, choose **Voice** > **VoIP Basic Configuration**.

b. In the right pane, configure the parameters of voice user 1 as follows:

- Line Name: A0
- Associated POTS: 1 (binding port TEL1 on the ONU)

Copyright © Huawei Technologies Co., Ltd.

- Select **Enable Line Name** to enable the voice user configuration.

c. Click **Apply** to apply the configuration.

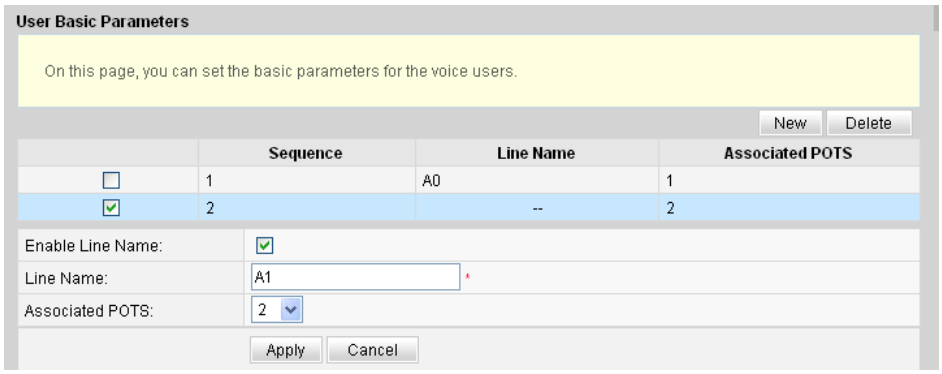
d. In the right pane, click **New** to add voice user 2, and configure the parameters of voice user 2 as follows:

- Line Name: A1
- Associated POTS: 2 (binding port TEL2 on the ONU)
- Select **Enable Line Name** to enable the voice user configuration.

e. Click **Apply** to apply the configuration.

NOTE

- The terminal IDs **A0** and **A1** must be consistent with the corresponding configuration on the MGC.
- If **Associated POTS** is **1**, port TEL1 on the ONU is bound. If **Associated POTS** is **2**, port TEL2 on the ONU is bound.



5. (Optional) Configure a route.

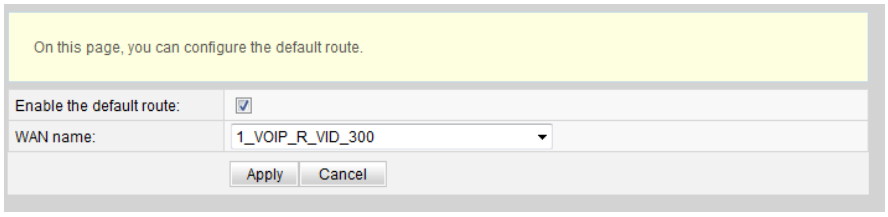
Perform this operation if the IP address of the ONU and the IP address of the voice server are in different network segments.

a. Choose **Route** > **Default Route Configuration** from the main menu.

b. Select **Enable the default route** and set **WAN name** to **1_VOIP_R_VID_300**.

Figure 12-11 shows the settings.

Figure 12-11 Configuring a route

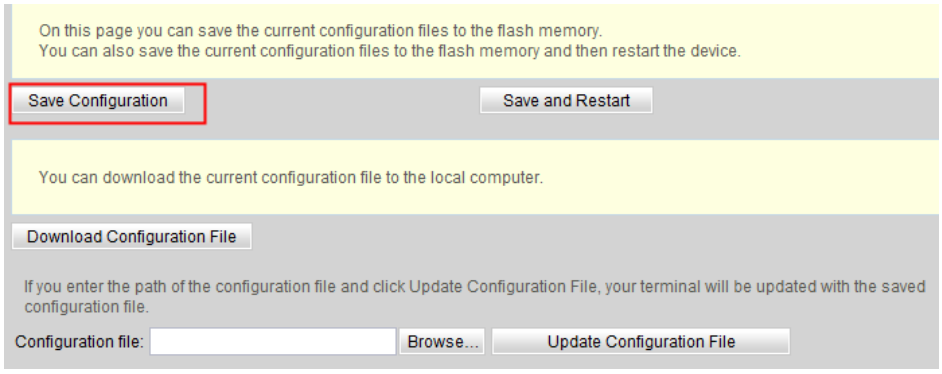


c. Click **Apply** to apply the configuration.

6. Save the configuration.

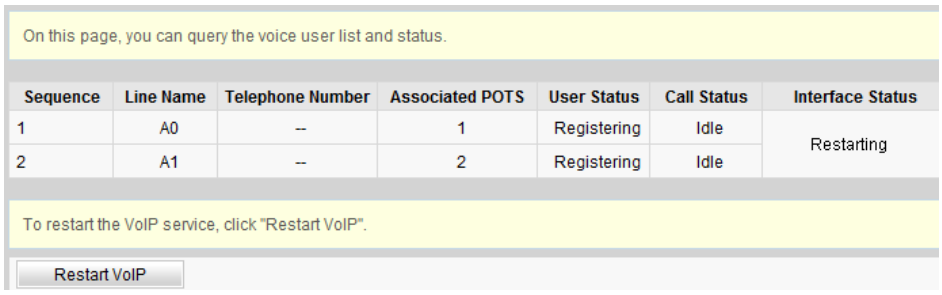
In the navigation tree, choose **System Tools** > **Configuration File**. In the right pane, click **Save Configuration** to save the configuration.

Copyright © Huawei Technologies Co., Ltd.



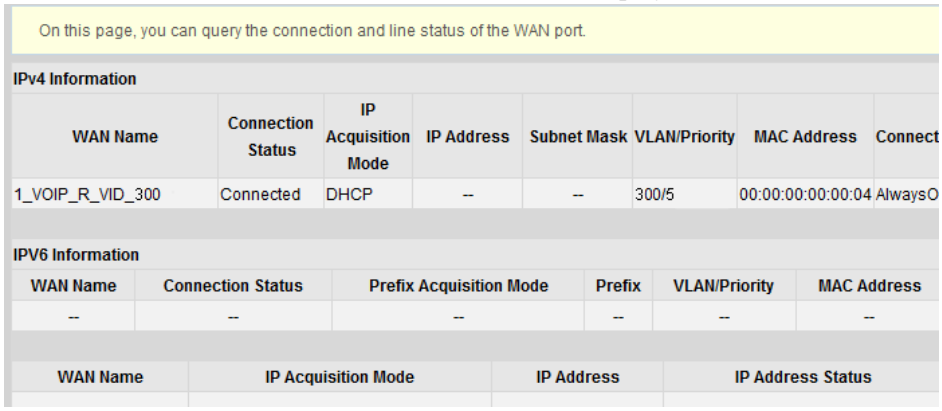
7. Restart the voice process.

   In the navigation tree, choose **Status** > **VoIP Information**. In the right pane, click **Restart VoIP**.



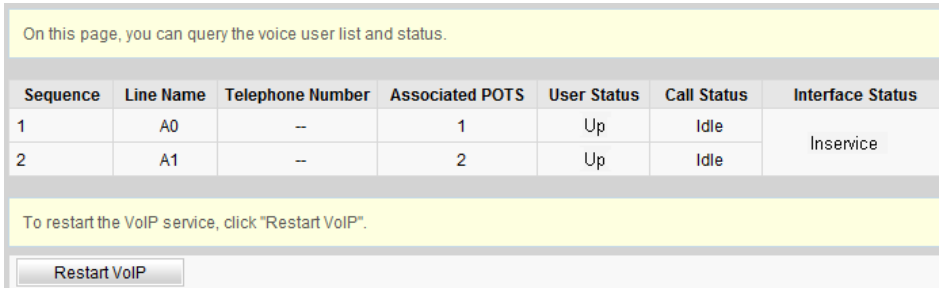
8. Check the ONU connection status.

   In the navigation tree, choose **Status** > **WAN Information**. In the right pane, **Status** is **Connected** and the obtained IP address is displayed at **IP Address**.



9. Check the registration status of a voice user.

   In the navigation tree, choose **Status** > **VoIP Information**. In the right pane, **User Status** is **Up**.



----End

Copyright © Huawei Technologies Co., Ltd.

12.4.2.6 Configuring the H.248-based Voice Service (Through the CLI)

The OLT manages ONUs and applies VoIP configurations to the ONU using the OMCI protocol. This topic describes how to configure the H.248-based voice service.

Prerequisite

- The interface data and POTS port data corresponding to the MG interface have been configured on the MGC.
- The OLT has been connected to the MGC. The OLT can ping the IP address of the MGC server successfully.
- The ONU has been added to the OLT. For details, see **12.3.3 Adding an ONU to an OLT**.
- Different voice services require different ONU software versions. Before the configuration, ensure that the ONU software version supports H.248. For details, see relevant ONU manuals.

Context

Table 12-39 Data plan

Item	Data
ONU line profile	Profile name: ftto_line T-CONT ID: 4 GEM port ID: 12
ONU service profile	Profile name: ftto_ser ONU port capability set: adaptive
Networking data	IP address of the MGC server: 200.200.200.200/24 Port ID of the MGC server: 2944

Procedure

Step 1 Configure a traffic profile.

Set the profile name to **ftto_voip** and do not limit the upstream and downstream rates. Set the priority to **5** and packets are scheduled according to the priority carried.

Run the **display traffic table ip** command to query existing traffic profiles in the system. If the existing traffic profiles in the system do not meet the requirements, run the **traffic table ip** command to add a traffic profile.

Step 2 Configure the mapping between a GEM port and a VLAN. Create a service VLAN and a service flow.

Copyright © Huawei Technologies Co., Ltd.

Table 12-40 Scenario plan

Scenario	VLAN Plan	VLAN Translation Policy
Scenario 1	Single VLAN tag ● S-VLAN ID: 300 ● S-VLAN type: smart ● S-VLAN attribute: common ● C-VLAN ID: 300	ONU: Configure a VLAN for all ONUs and add the same C-VLAN tag to packets. All ONUs are in the same C-VLAN. OLT: The OLT transparently transmits VLAN tags (the C-VLAN is the same as the planned S-VLAN).
Scenario 2	Single VLAN tag ● S-VLAN ID: 300 ● S-VLAN type: smart ● S-VLAN attribute: common ● C-VLAN ID: 3001	ONU: Configure a VLAN for all ONUs and add the same C-VLAN tag to packets. All ONUs are in the same C-VLAN. OLT: The OLT switches between C-VLAN tags and S-VLAN tags (C-VLAN is different from the planned S-VLAN).

Scenario 1:

Configure the mapping between a GEM port and a VLAN. The service flow of user VLAN 300 is mapped to GEM port 12 in the ONU line profile.

```
huawei(config)#ont-lineprofile gpon profile-name ftto_line
huawei(config-gpon-lineprofile-1)#gem mapping 12 2 vlan 300
huawei(config-gpon-lineprofile-1)#commit
huawei(config-gpon-lineprofile-1)#quit
```

Create a service VLAN and add an upstream port to it. Add upstream port 0/19/0 to VLAN 300.

```
huawei(config)#vlan 300 smart
huawei(config)#port vlan 300 0/19 0
```

Create service flows. Set the service VLAN to 300, GEM port ID to 12, and user VLAN to 300, and use traffic profile **ftto_voip**.

```
huawei(config)#service-port vlan 300 gpon 0/1/0 ont 1 gemport 12 multi-service
 user-vlan 300 inbound traffic-table name ftto_voip outbound traffic-table name
ftto_voip
huawei(config)#service-port vlan 300 gpon 0/1/0 ont 2 gemport 12 multi-service
 user-vlan 300 inbound traffic-table name ftto_voip outbound traffic-table name
ftto_voip
```

Scenario 2:

Configure the mapping between a GEM port and a VLAN. The service flow of user VLAN 3001 is mapped to GEM port 12 in the ONU line profile.

```
huawei(config)#ont-lineprofile gpon profile-name ftto_line
huawei(config-gpon-lineprofile-1)#gem mapping 12 2 vlan 3001
huawei(config-gpon-lineprofile-1)#commit
huawei(config-gpon-lineprofile-1)#quit
```


Copyright © Huawei Technologies Co., Ltd.

Create a service VLAN and add an upstream port to it. Add upstream port 0/19/0 to VLAN 300.

```
huawei(config)#vlan 300 smart
huawei(config)#vlan attrib 300 stacking
huawei(config)#port vlan 300 0/19 0
```

Create service flows. Set the service VLAN to 300, GEM port ID to 12, and user VLAN to 3001. Use traffic profile **ftto_voip**.

```
huawei(config)#service-port vlan 300 gpon 0/1/0 ont 1 gemport 12 multi-service
user-vlan 3001 tag-transform translate inbound traffic-table name ftto_voip
outboun
d traffic-table name ftto_voip
huawei(config)#service-port vlan 300 gpon 0/1/0 ont 2 gemport 12 multi-service
user-vlan 3001 tag-transform translate inbound traffic-table name ftto_voip
outboun
d traffic-table name ftto_voip
```

Step 3 Configure ONU voice service profiles.

ONU voice service profiles include the interface common profile, MGC interface profile, and POTS port profile.

- Interface common profile: saves common attributes of an ONU voice interface, including the fax mode, fax/modem negotiation mode, and priority of the coding and decoding mode.
- MGC interface profile: saves the IP address or domain name of the MGC, protocol port ID of the MGC transport layer to which the MG interface belongs, and DSCP priority of media packets.
- POTS port profile: saves physical attributes of a POTS port on an ONU, including the impedance, transmitting gain, receiving gain, and signaling type of the POTS port.

1. Configure an interface common profile.

   Run the **display ont-mg-attribute-profile** command to query the existing interface common profile in the system. If the existing interface common profile in the system does not meet the requirements, run the **ont-mg-attribute-profile add** command to add an interface common profile.

   In this example, the default interface common profile, namely interface common profile 1 is used.

2. Configure an MGC interface profile.

   Run the **display ont-mgc-profile** command to query the existing MGC interface profile in the system. If the existing MGC interface profile in the system does not meet the requirements, run the **ont-mgc-profile add** command to add an MGC interface profile.

   Create MGC interface profile 2, set the IP address of the MGC to 200.200.200.200, and use default values for other parameters.

   ```
   huawei(config)#ont-mgc-profile add profile-id 2 primary-mgc 200.200.200.200
   ```

3. Configure a POTS port profile.

   Run the **display ont-pots-profile** command to query the existing POTS port profile in the system. If the existing POTS port profile in the system does not meet the requirements, run the **ont-pots-profile add** command to add a POTS port profile.

   In this example, the default POTS port profile, namely POTS port profile 1 is used.

Step 4 Configure the IP addresses of ONU SIP users.

For ONU 1 and ONU 2, configure the IP address obtaining mode to the static mode, set the IP addresses to 10.10.10.10/24 and 10.10.10.20/24, set the management VLAN to VLAN 20, and use default values for other parameters.

Copyright © Huawei Technologies Co., Ltd.

```
huawei(config)#interface gpon 0/1
huawei(config-if-gpon-0/1)#ont ipconfig 0 1 dhcp vlan 20
huawei(config-if-gpon-0/1)#ont ipconfig 0 2 dhcp vlan 20
```

Step 5 Configure H.248 POTS users.

1. Add an H.248 interface and apply an MGC interface profile to the interface.

   For ONU 1 and ONU 2, set the MG ID to 1, apply MGC interface profile 2 to ONU 1 and ONU 2, and use default values for other parameters.

   If parameters of an MGC interface profile are changed, the MGC interface profile must be reapplied to the ONU so that the changed parameters can take effect.

   ```
   huawei(config-if-gpon-0/1)#if-h248 add 0 1 1 mgc-profile profile-id 2
   huawei(config-if-gpon-0/1)#if-h248 add 0 2 1 mgc-profile profile-id 2
   ```

2. Add POTS users.

   For ONU 1 and ONU 2, create a POTS user, set the MG ID to 1 (identical to the MG ID of the H.248 interface), and set the physical terminal port ID to A0 and A1.

   ```
   huawei(config-if-gpon-0/1)#mgpstnuser add 0 1 1 mgid 1 terminalid A0
   huawei(config-if-gpon-0/1)#mgpstnuser add 0 2 1 mgid 1 terminalid A1
   ```

   Run the **display mgpstnuser attribute** command to check whether the configuration of the POTS user is properly set.

   ```
   huawei(config-if-gpon-0/1)#display mgpstnuser attribute 0 1 1

   ---------------------------------------------------------------------------
     F/S/P                       : 0/1/0
     ONT ID                      : 1
     Port ID                     : 1

     MG ID                       : 1
     Terminal ID                 : A0
   ...//The rest of the response information is omitted.

   huawei(config-if-gpon-0/1)#display mgpstnuser attribute 0 2 1

   ---------------------------------------------------------------------------
     F/S/P                       : 0/1/0
     ONT ID                      : 2
     Port ID                     : 1

     MG ID                       : 1
     Terminal ID                 : A1
   ...//The rest of the response information is omitted.
   ```

Step 6 Apply ONU voice service profiles

After ONU voice service profiles are applied, if parameters in those profiles are changed, those profiles must be reapplied so that the changed parameters can take effect.

1. Apply an interface common profile.

   Run the **if-h248 attribute** command to apply an interface common profile to an H.248 interface or configure the interface customized parameters, or run the **ont-if-h248 bat-apply** command to bulk apply the interface common profiles to H.248 interfaces. If you use these two commands to apply the interface common profiles or configure the interface customized parameters repeatedly, the last configurations take effect.

   In this example, the default interface common profile, namely interface common profile 1 is used.

2. Apply a POTS port profile.

Copyright © Huawei Technologies Co., Ltd.

Run the **pstnport electric** command to apply a POTS port profile to an H.248 interface or configure the interface customized parameters, or run the **ont-pstnport electric bat-apply** command to bulk apply the POTS port profiles to H.248 interfaces. If you use these two commands to apply the POTS port profiles or configure the interface customized parameters repeatedly, the last configurations take effect.

In this example, the default POTS port profile, namely POTS port profile 1 is used.

Step 7 (Optional) Configure the H.248 user codec.

Run the **mgpstnuser codec** command to configure the H.248 user codec. The H.248 user codec will not be configured independently in this example.

Step 8 Save the data.

```
huawei(config)#save
```

----End

12.4.2.7 Configuring the SIP-based Voice Service (on a Web Page)

The OLT is connected to the remote ONU through a GPON port to provide users with the IP-based high-quality and low-cost VoIP service.

Prerequisite

- The SIP interface data and POTS port data corresponding to the MG interface have been configured on the SIP server.
- The connection between the OLT and the SIP server is set up. The OLT can ping the IP address of the SIP server successfully.
- The ONU has been added to the OLT. For details, see **9.7.1.3 Adding an ONT to an OLT**.
- Different voice services require different ONU software versions. Before the configuration, ensure that the current ONU software version supports SIP. For details, see relevant ONU manuals.

Data Plan

Table 12-41 Data plan

Item	Data
ONU line profile	Profile name: ftto_line T-CONT ID: 4 GEM port ID: 12
ONU service profile	Profile name: ftto_ser ONU port capability set: adaptive

Copyright © Huawei Technologies Co., Ltd.

Item	Data
Voice parameter	IP address of the SIP server: 200.200.200.200/24 Port ID of the SIP server: 5060 Home domain name: huawei.com User phone number 1: 77730010 User phone number 2: 77730020

Procedure

- Configure the OLT.
  1. Configure a traffic profile.

     Set the profile name to **ftto_voip** and do not limit the upstream and downstream rates. Set the priority to **5** and packets are scheduled according to the priority carried.

     Run the **display traffic table ip** command to query existing traffic profiles in the system. If the existing traffic profiles in the system do not meet the requirements, run the **traffic table ip** command to add a traffic profile.

     ```
     huawei(config)#traffic table ip name ftto_voip cir off priority 5 priority-policy
      local-setting
     ```

  2. Configure the mapping between a GEM port and a VLAN. Create a service VLAN and a service flow.

     Table 12-42 Scenario plan

Scenario	VLAN Plan	VLAN Translation Policy
Scenario 1	Single VLAN tag ● S-VLAN ID: 300 ● S-VLAN type: smart ● S-VLAN attribute: common ● C-VLAN ID: 300	ONU: Configure a VLAN for all ONUs and add the same C-VLAN tag to packets. All ONUs are in the same C-VLAN. OLT: The OLT transparently transmits VLAN tags (the C-VLAN is the same as the planned S-VLAN).

Copyright © Huawei Technologies Co., Ltd.

Scenario	VLAN Plan	VLAN Translation Policy
Scenario 2	Single VLAN tag ● S-VLAN ID: 300 ● S-VLAN type: smart ● S-VLAN attribute: common ● C-VLAN ID: 3001	ONU: Configure a VLAN for all ONUs and add the same C-VLAN tag to packets. All ONUs are in the same C-VLAN. OLT: The OLT switches between C-VLAN tags and S-VLAN tags (C-VLAN is different from the planned S-VLAN).

Scenario 1:

Configure the mapping between a GEM port and a VLAN. The service flow of user VLAN 300 is mapped to GEM port 12 in the ONU line profile.

```
huawei(config)#ont-lineprofile gpon profile-name ftto_line
huawei(config-gpon-lineprofile-1)#gem mapping 12 2 vlan 300
huawei(config-gpon-lineprofile-1)#commit
huawei(config-gpon-lineprofile-1)#quit
```

Create a service VLAN and add an upstream port to it. Add upstream port 0/19/0 to VLAN 300.

```
huawei(config)#vlan 300 smart
huawei(config)#port vlan 300 0/19 0
```

Create service flows. Set the service VLAN to 300, GEM port ID to 12, and user VLAN to 300, and use traffic profile **ftto_voip**.

```
huawei(config)#service-port vlan 300 gpon 0/1/0 ont 1 gemport 12 multi-
service
 user-vlan 300 inbound traffic-table name ftto_voip outbound traffic-table
name
ftto_voip
huawei(config)#service-port vlan 300 gpon 0/1/0 ont 2 gemport 12 multi-
service
 user-vlan 300 inbound traffic-table name ftto_voip outbound traffic-table
name
ftto_voip
```

Scenario 2:

Configure the mapping between a GEM port and a VLAN. The service flow of user VLAN 3001 is mapped to GEM port 12 in the ONU line profile.

```
huawei(config)#ont-lineprofile gpon profile-name ftto_line
huawei(config-gpon-lineprofile-1)#gem mapping 12 2 vlan 3001
huawei(config-gpon-lineprofile-1)#commit
huawei(config-gpon-lineprofile-1)#quit
```

Create a service VLAN and add an upstream port to it. Add upstream port 0/19/0 to VLAN 300.

```
huawei(config)#vlan 300 smart
huawei(config)#vlan attrib 300 stacking
huawei(config)#port vlan 300 0/19 0
```


Copyright © Huawei Technologies Co., Ltd.

Create service flows. Set the service VLAN to 300, GEM port ID to 12, and user VLAN to 3001. Use traffic profile **ftto_voip**.

```
huawei(config)#service-port vlan 300 gpon 0/1/0 ont 1 gemport 12 multi-
service
user-vlan 3001 tag-transform translate inbound traffic-table name
ftto_voip outboun
d traffic-table name ftto_voip
huawei(config)#service-port vlan 300 gpon 0/1/0 ont 2 gemport 12 multi-
service
user-vlan 3001 tag-transform translate inbound traffic-table name
ftto_voip outboun
d traffic-table name ftto_voip
```

3. Enable the ARP proxy function.

   Voice media streams for different users of the same S-VLAN fail to interchange because the service ports of the smart VLAN are isolated from each other. Therefore, the ARP proxy function needs to be enabled on the OLT.

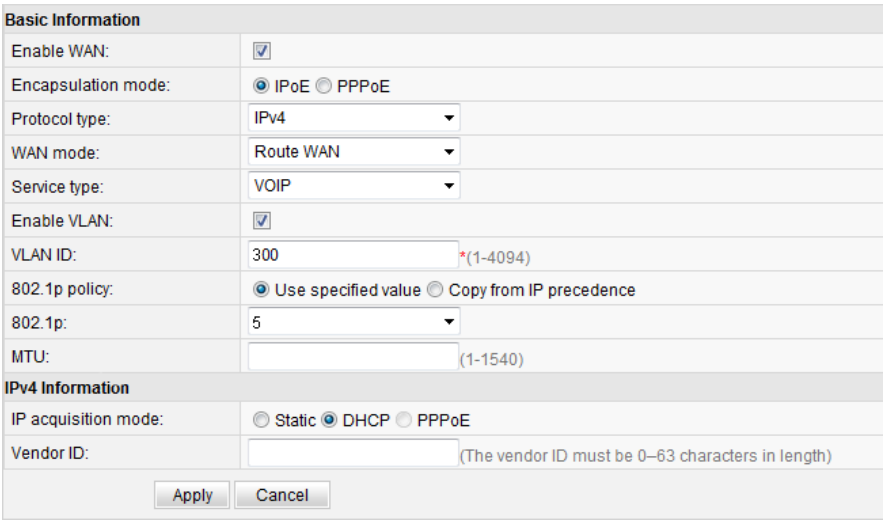
   ```
   huawei(config)#arp proxy enable
   huawei(config)#interface vlanif 300
   huawei(config-if-vlanif300)#arp proxy enable
   huawei(config-if-vlanif300)#quit
   ```

4. Save the data.

   ```
   huawei(config)#save
   ```

- Configure the ONU on the Web page.
  1. Log in to the Web configuration window.
     a. Configure the IP address of the PC network adapter to be in the same network segment as the IP address of the local maintenance Ethernet port on the ONU (default: **192.168.100.1**).
     b. Open the Web browser, and enter the IP address of the local maintenance Ethernet port of the ONU.
     c. On the login window, enter the user name (default: **telecomadmin**) and password (default: **admintelecom**) of the administrator. After the password authentication is passed, the Web configuration interface is displayed.
  2. Configure parameters of a voice WAN port.
     a. In the navigation tree, choose **WAN** > **WAN Configuration**.
     b. In the right pane, click **New**. In the dialog box that is displayed, configure parameters of a WAN port as follows:
        - WAN Connection: Enable
        - Service List: VoIP (For configuring the VoIP service, VoIP or a combination containing VoIP needs to be selected.)
        - Mode: Route
        - VLAN ID: 300 (The VLAN ID of the ONU must be the same as the user-side VLAN ID configured on the OLT.)
        - 802.1p: 5
        - IP Acquisition Mode: DHCP

Copyright © Huawei Technologies Co., Ltd.



c. Click **Apply** to apply the configuration.

3. Configure parameters of the SIP-based voice interface.

a. In the navigation tree, choose **Voice** > **VoIP Basic Configuration**.

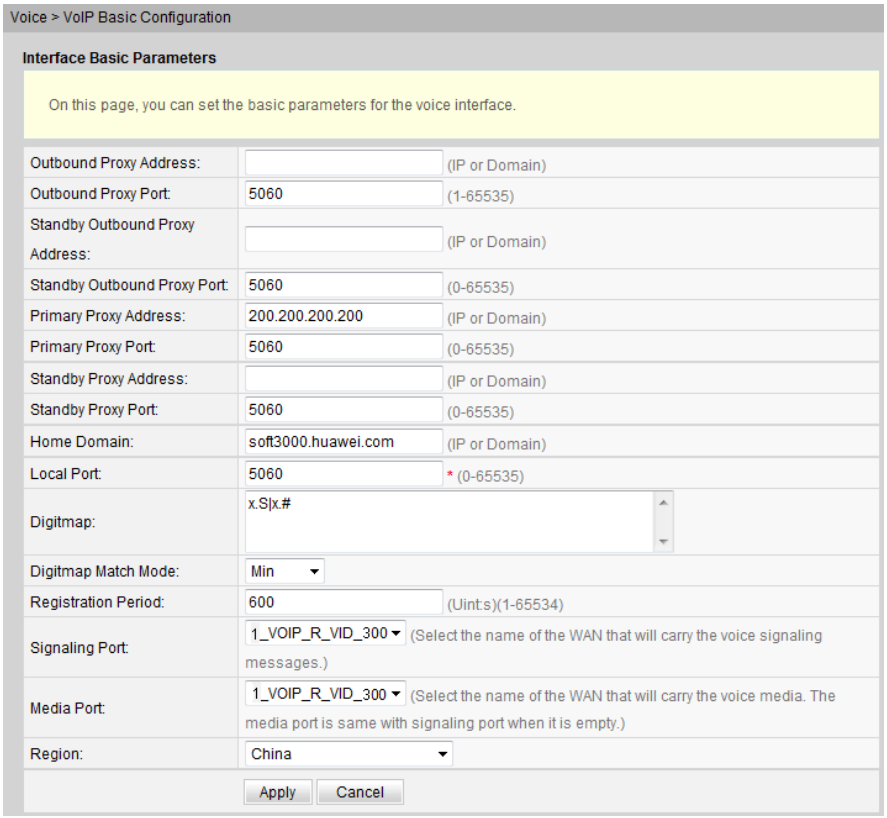
b. In the right pane, configure parameters of the SIP-based voice interface as follows (other parameters use the default settings):

- Set **Proxy Server Address** below **Primary Server** to **200.200.200.200**.
- Home Domain: softx3000.huawei.com
- Signaling Port: 1_VOIP_R_VID_300
- Region: China

NOTE

- The parameters of the SIP-based voice interface must be consistent with the corresponding configuration on the softswitch.
- If dual-homing is configured, **Proxy Server Address** below **Secondary Server** must be configured.
- If **Signaling Port** is empty, the parameter value is the same as **Media Port**. If the upper-layer network requires isolation of media streams from signaling streams, create different traffic streams for the media streams and signaling streams on the OLT, create different WAN ports on the ONU, and bind the created WAN ports to **Media Port** and **Signaling Port**. When the packet is forwarded from two WAN ports, the configured VLAN is carried by default.

Copyright © Huawei Technologies Co., Ltd.



c. Click **Apply** to apply the configuration.

4. Configure parameters of the SIP-based voice users.

a. In the navigation tree, choose **Voice** > **VoIP Basic Configuration**.

b. In the right pane, configure parameters of voice user 1 as follows:

- Register User Name: 80001234
- Auth User Name: 80001234@softx3000.huawei.com
- Password: iadtest1
- Associated POTS: 1 (binding port TEL1 on the ONU)
- Select **Enable** to enable the voice user configuration.

c. Click **Apply** to apply the configuration.

d. Register User Name: 80001235

e. Auth User Name: 80001235@softx3000.huawei.com

f. Password: iadtest2

g. Associated POTS: 2 (binding port TEL2 on the ONU)

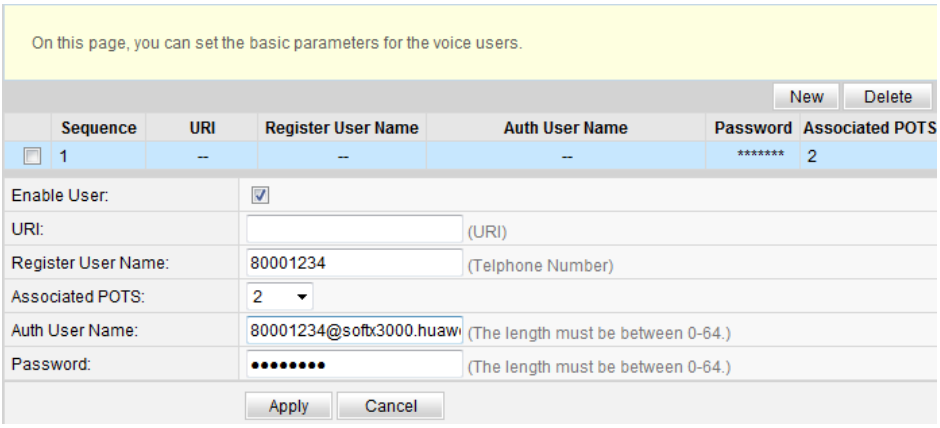
h. Select **Enable User** to enable the voice user configuration.

i. Click **Apply** to apply the configuration.

NOTE

- The parameters of the SIP-based voice user must be consistent with the corresponding configuration on the softswitch.
- If **Associated POTS** is **1**, port TEL1 on the ONU is bound. If **Associated POTS** is **2**, port TEL2 on the ONU is bound.

Copyright © Huawei Technologies Co., Ltd.



5. (Optional) Configure a route.

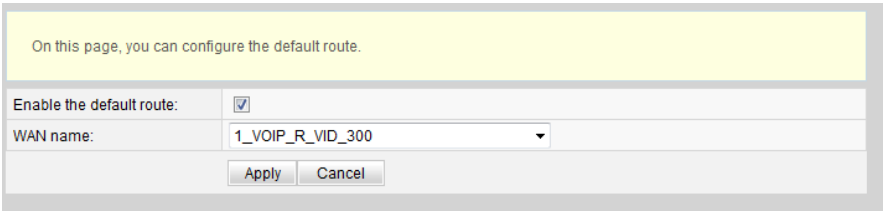
   Perform this operation if the IP address of the ONU and the IP address of the voice server are in different network segments.

   a. Choose **Route** > **Default Route Configuration** from the main menu.

   b. Select **Enable the default route** and set **WAN name** to **1_VOIP_R_VID_300**.

      Figure 12-12 shows the settings.

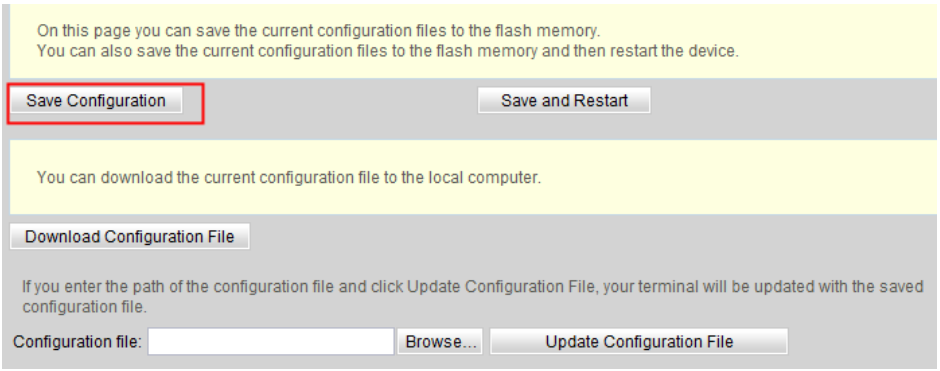
      Figure 12-12 Configuring a route

   c. Click **Apply** to apply the configuration.

6. Save the configuration.

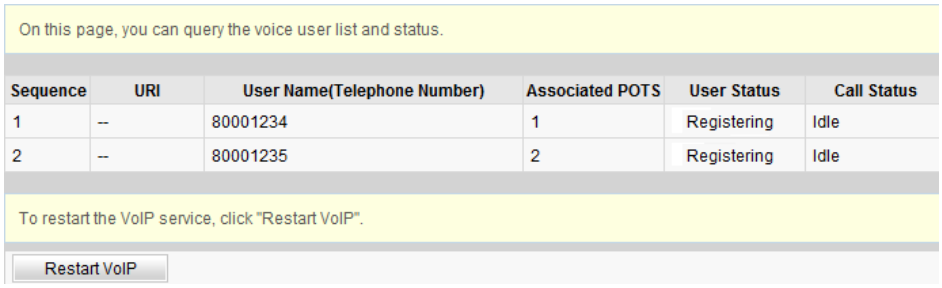
   In the navigation tree, choose **System Tools** > **Configuration File**. In the right pane, click **Save Configuration** to save the configuration.

7. Restart the voice process.

   In the navigation tree, choose **Status** > **VoIP Information**. In the right pane, click **Restart VoIP**.

Copyright © Huawei Technologies Co., Ltd.


On this page, you can query the voice user list and status.

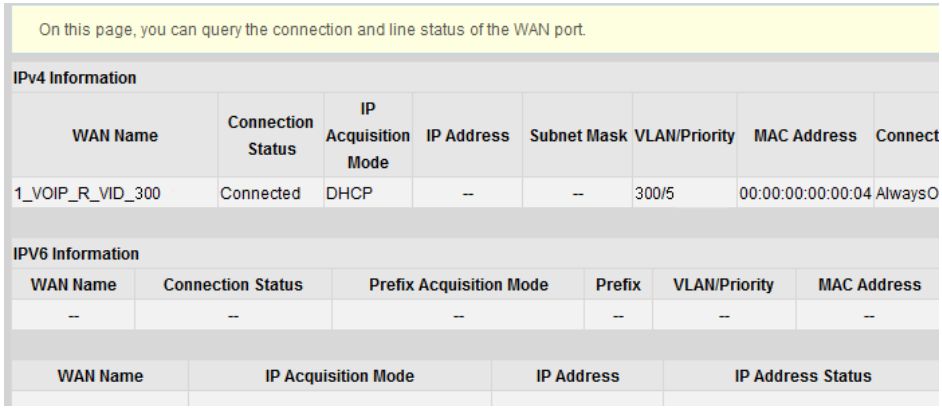
Sequence	URI	User Name(Telephone Number)	Associated POTS	User Status	Call Status
1	--	80001234	1	Registering	Idle
2	--	80001235	2	Registering	Idle

To restart the VoIP service, click "Restart VoIP".

Restart VoIP

8. Check the ONU connection status.

   In the navigation tree, choose **Status** > **WAN Information**. In the right pane, **Status** is **Connected** and the obtained IP address is displayed at **IP Address**.


On this page, you can query the connection and line status of the WAN port.

IPv4 Information

WAN Name	Connection Status	IP Acquisition Mode	IP Address	Subnet Mask	VLAN/Priority	MAC Address	Connect
1_VOIP_R_VID_300	Connected	DHCP	--	--	300/5	00:00:00:00:00:04	AlwaysO

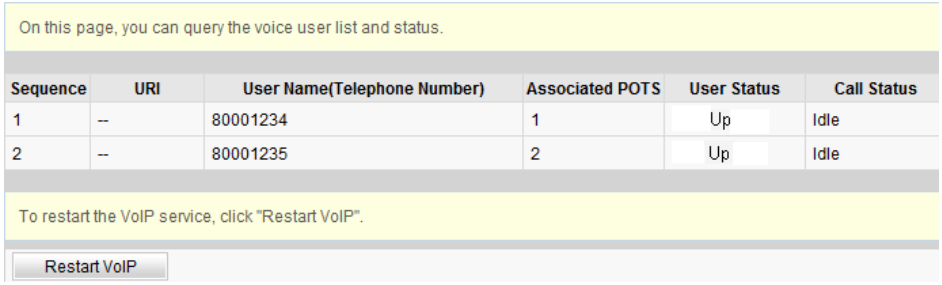
IPV6 Information

WAN Name	Connection Status	Prefix Acquisition Mode	Prefix	VLAN/Priority	MAC Address
--	--	--	--	--	--

WAN Name	IP Acquisition Mode	IP Address	IP Address Status

9. Check the registration status of the voice user.

   In the navigation tree, choose **Status** > **VoIP Information**. In the right pane, **User Status** is **Up**.


On this page, you can query the voice user list and status.

Sequence	URI	User Name(Telephone Number)	Associated POTS	User Status	Call Status
1	--	80001234	1	Up	Idle
2	--	80001235	2	Up	Idle

To restart the VoIP service, click "Restart VoIP".

Restart VoIP

----End

12.4.2.8 Configuring the SIP-based Voice Service (Through the CLI)

The OLT manages ONUs and applies VoIP configurations to the ONU using the OMCI protocol. This topic describes how to configure the SIP-based voice service.

Prerequisite

- The SIP interface data and POTS port data corresponding to the MG interface have been configured on the SIP server.
- The connection between the OLT and the SIP server is set up. The OLT can ping the IP address of the SIP server successfully.

Copyright © Huawei Technologies Co., Ltd.

- The ONU has been added to the OLT. For details, see **9.7.1.3 Adding an ONT to an OLT**.
- Different voice services require different ONU software versions. Before the configuration, ensure that the current ONU software version supports SIP. For details, see relevant ONU manuals.

Data Plan

Table 12-43 Data plan

Item	Data
ONU line profile	Profile name: ftto_line T-CONT ID: 4 GEM port ID: 12
ONU service profile	Profile name: ftto_ser ONU port capability set: adaptive
Voice parameter	IP address of the SIP server: 200.200.200.200/24 Port ID of the SIP server: 5060 Home domain name: huawei.com User phone number 1: 77730010 User phone number 2: 77730020

Procedure

Step 1 Configure a traffic profile.

Set the profile name to **ftto_voip** and do not limit the upstream and downstream rates. Set the priority to **5** and packets are scheduled according to the priority carried.

Run the **display traffic table ip** command to query existing traffic profiles in the system. If the existing traffic profiles in the system do not meet the requirements, run the **traffic table ip** command to add a traffic profile.

Step 2 Configure the mapping between a GEM port and a VLAN. Create a service VLAN and a service flow.

Copyright © Huawei Technologies Co., Ltd.

Table 12-44 Scenario plan

Scenario	VLAN Plan	VLAN Translation Policy
Scenario 1	Single VLAN tag ● S-VLAN ID: 300 ● S-VLAN type: smart ● S-VLAN attribute: common ● C-VLAN ID: 300	ONU: Configure a VLAN for all ONUs and add the same C-VLAN tag to packets. All ONUs are in the same C-VLAN. OLT: The OLT transparently transmits VLAN tags (the C-VLAN is the same as the planned S-VLAN).
Scenario 2	Single VLAN tag ● S-VLAN ID: 300 ● S-VLAN type: smart ● S-VLAN attribute: common ● C-VLAN ID: 3001	ONU: Configure a VLAN for all ONUs and add the same C-VLAN tag to packets. All ONUs are in the same C-VLAN. OLT: The OLT switches between C-VLAN tags and S-VLAN tags (C-VLAN is different from the planned S-VLAN).

Scenario 1:

Configure the mapping between a GEM port and a VLAN. The service flow of user VLAN 300 is mapped to GEM port 12 in the ONU line profile.

```
huawei(config)#ont-lineprofile gpon profile-name ftto_line
huawei(config-gpon-lineprofile-1)#gem mapping 12 2 vlan 300
huawei(config-gpon-lineprofile-1)#commit
huawei(config-gpon-lineprofile-1)#quit
```

Create a service VLAN and add an upstream port to it. Add upstream port 0/19/0 to VLAN 300.

```
huawei(config)#vlan 300 smart
huawei(config)#port vlan 300 0/19 0
```

Create service flows. Set the service VLAN to 300, GEM port ID to 12, and user VLAN to 300, and use traffic profile **ftto_voip**.

```
huawei(config)#service-port vlan 300 gpon 0/1/0 ont 1 gemport 12 multi-service
 user-vlan 300 inbound traffic-table name ftto_voip outbound traffic-table name
ftto_voip
huawei(config)#service-port vlan 300 gpon 0/1/0 ont 2 gemport 12 multi-service
 user-vlan 300 inbound traffic-table name ftto_voip outbound traffic-table name
ftto_voip
```

Scenario 2:

Configure the mapping between a GEM port and a VLAN. The service flow of user VLAN 3001 is mapped to GEM port 12 in the ONU line profile.

```
huawei(config)#ont-lineprofile gpon profile-name ftto_line
huawei(config-gpon-lineprofile-1)#gem mapping 12 2 vlan 3001
huawei(config-gpon-lineprofile-1)#commit
huawei(config-gpon-lineprofile-1)#quit
```


Copyright © Huawei Technologies Co., Ltd.

Create a service VLAN and add an upstream port to it. Add upstream port 0/19/0 to VLAN 300.

```
huawei(config)#vlan 300 smart
huawei(config)#vlan attrib 300 stacking
huawei(config)#port vlan 300 0/19 0
```

Create service flows. Set the service VLAN to 300, GEM port ID to 12, and user VLAN to 3001. Use traffic profile **ftto_voip**.

```
huawei(config)#service-port vlan 300 gpon 0/1/0 ont 1 gemport 12 multi-service
user-vlan 3001 tag-transform translate inbound traffic-table name ftto_voip
outboun
d traffic-table name ftto_voip
huawei(config)#service-port vlan 300 gpon 0/1/0 ont 2 gemport 12 multi-service
user-vlan 3001 tag-transform translate inbound traffic-table name ftto_voip
outboun
d traffic-table name ftto_voip
```

Step 3 Configure ONU voice service profiles.

ONU voice service profiles include the interface common profile, SIP agent profile, SIP service data profile, POTS port profile, and digitmap profile.

- Interface common profile: saves common attributes of an ONU voice interface, including the fax mode, fax/modem negotiation mode, and priority of the coding and decoding mode.
- SIP agent profile: saves the SIP agent information about an ONU, including the IP address and domain name of the SIP agent server and attributes of media packets and signaling packets.
- SIP service data profile: saves the data information about ONU voice services, including the rights of the call waiting service, three-party service, call forwarding service, and call holding service.
- POTS port profile: saves physical attributes of a POTS port on an ONU, including the impedance, transmitting gain, receiving gain, and signaling type of the POTS port.
- Digitmap profile: saves the digitmap information about an ONU, including the timeout time of the digitmap timer and the digitmap format.

1. Configure an interface common profile.

   Run the **display ont-mg-attribute-profile** command to query the existing interface common profile in the system. If the existing interface common profile in the system does not meet the requirements, run the **ont-mg-attribute-profile add** command to add an interface common profile.

   In this example, the default interface common profile, namely interface common profile 1 is used.

2. Configure an SIP agent profile.

   Run the **display ont-sipagent-profile** command to query the existing SIP agent profile in the system. If the existing SIP agent profile in the system does not meet the requirements, run the **ont-sipagent-profile add** command to add an SIP agent profile.

   Create SIP agent profile 2, set the IP address of the SIP server to 200.200.200.200, and use default values for other parameters.

   ```
   huawei(config)#ont-sipagent-profile add profile-id 2 proxy-server
   200.200.200.200
   ```

3. Configure an SIP service data profile.

   Run the **display ont-siprightflag-profile** command to query the existing SIP agent profile in the system. If the existing SIP service data profile in the system does not meet the requirements, run the **ont-siprightflag-profile add** command to add an SIP service data profile.

Copyright © Huawei Technologies Co., Ltd.

In this example, the default SIP service data profile, namely SIP service data profile 1 is used.

4. Configure a POTS port profile.

   Run the **display ont-pots-profile** command to query the existing POTS port profile in the system. If the existing POTS port profile in the system does not meet the requirements, run the **ont-pots-profile add** command to add a POTS port profile.

   In this example, the default POTS port profile, namely POTS port profile 1 is used.

5. Configure a digitmap profile.

   Run the **display ont-digitmap-profile** command to query the existing digitmap profile in the system. If the existing digitmap profile in the system does not meet the requirements, run the **ont-digitmap-profile add** command to add a digitmap profile.

   In this example, the default digitmap profile, namely digitmap profile 1 is used.

Step 4 Configure an IP address for an ONU SIP user.

For ONU 1 and ONU 2, configure the IP address obtaining mode to the DHCP mode, set the management VLAN to VLAN 20, and use default values for other parameters.

```
huawei(config)#interface gpon 0/1
huawei(config-if-gpon-0/1)#ont ipconfig 0 1 dhcp vlan 20
huawei(config-if-gpon-0/1)#ont ipconfig 0 2 dhcp vlan 20
```

Step 5 Configure SIP POTS users.

1. Add an SIP interface and apply an SIP agent profile to the interface.

   For ONU 1 and ONU 2, set the MG ID to 1, apply SIP agent profile 2 to ONU 1 and ONU 2, and use default values for other parameters.

   If parameters in an SIP agent profile are changed, the SIP agent profile must be reapplied to the ONU so that the changed parameters can take effect.

   ```
   huawei(config-if-gpon-0/1)#if-sip add 0 1 1 sipagent-profile profile-id 2
   huawei(config-if-gpon-0/1)#if-sip add 0 2 1 sipagent-profile profile-id 2
   ```

2. Add POTS users.

   For ONU 1 and ONU 2, set the MG ID to 1 (identical to the MG ID of the added SIP interface), create two POTS users named huawei1 and huawei2, set passwords to user1 and user2, set their phone numbers to 77730010 and 77730020 and use default values for other parameters.

   ```
   huawei(config-if-gpon-0/1)#sippstnuser add 0 1 1 mgid 1 username huawei1 telno
   77730010
   huawei(config-if-gpon-0/1)#sippstnuser add 0 2 1 mgid 1 username huawei2 telno
   77730020
   ```

   Run the **display sippstnuser attribute** command to check whether the configuration of the POTS user is properly set.

   ```
   huawei(config-if-gpon-0/1)#display sippstnuser attribute 0 1 1

   ------------------------------------------------------------------------------
     F/S/P                       : 0/1/0
     ONT ID                      : 1
     Port ID                     : 1

     MG ID                       : 1
     Telephone NO.               : 77730010
     User name                   : huawei1
     Password                    : user1
   ...//The rest of the response information is omitted.

   huawei(config-if-gpon-0/1)#display sippstnuser attribute 0 2 1
   ```


Copyright © Huawei Technologies Co., Ltd.

```
---------------------------------------------------------------------------
  F/S/P                         : 0/1/0
  ONT ID                        : 2
  Port ID                       : 1

  MG ID                         : 1
  Telephone NO.                 : 77730020
  User name                     : huawei2
  Password                      : user2
...//The rest of the response information is omitted.
```

Step 6 Apply and bind an ONU voice service profile to an SIP interface

Currently, the interface common profile, SIP agent profile, SIP service data profile, and POTS port profile can be applied to an SIP interface, and the digitmap profile can be bound to an SIP interface.

For profiles that can be applied to an SIP interface, if parameters in those profiles are changed, those profiles must be reapplied to the SIP interface so that the changed parameters can take effect. For profiles that can be bound to an SIP interface, if parameters in those profiles are changed, those profiles do not need to be rebound to the SIP interface and the changed parameters can take effect.

The method for applying an SIP agent profile is introduced in **Step 5.1**. The following will introduce the methods for applying an interface common profile, an SIP service data profile, and a POTS port profile, and the method for binding a digitmap to an SIP interface.

1. Apply an interface common profile.

   Run the **if-sip attribute** command to apply an interface common profile to an SIP interface or configure the interface customized parameters, or run the **ont-if-sip bat-apply from** command to bulk apply the interface common profiles to SIP interfaces. If you use these two commands to apply the interface common profiles or configure the interface customized parameters repeatedly, the last configurations take effect.

   In this example, the default interface common profile, namely interface common profile 1 is used.

2. Apply an SIP service data profile.

   Run the **sippstnuser rightflag** command to apply an SIP service data profile to an SIP interface or configure the interface customized parameters, or run the **ont-sippstnuser bat-apply from** command to bulk apply the SIP service data profiles to SIP interfaces. If you use these two commands to apply the SIP service data profiles or configure the interface customized parameters repeatedly, the last configurations take effect.

   In this example, the default SIP service data profile, namely SIP service data profile 1 is used.

3. Apply a POTS port profile.

   Run the **pstnport electric** command to apply a POTS port profile to an SIP interface or configure the interface customized parameters, or run the **ont-pstnport electric bat-apply** command to bulk apply the POTS port profiles to SIP interfaces. If you use these two commands to apply the POTS port profiles or configure the interface customized parameters repeatedly, the last configurations take effect.

   In this example, the default POTS port profile, namely POTS port profile 1 is used.

4. Bind a digitmap profile.

   Run the **sippstnuser digitmap** command to bind a digitmap profile to an SIP interface, or run the **ont-sippstnuser bat-bind from** command to bulk apply the digitmap profiles to

Copyright © Huawei Technologies Co., Ltd.

SIP interfaces. If you use these two commands to bind the SIP service data profiles to SIP ports repeatedly, the last configurations take effect.

In this example, the default digitmap profile, namely digitmap profile 1 is used.

Step 7 (Optional) Configure the SIP user codec.

Run the **sippstnuser codec** command to configure the SIP user codec. The SIP user codec will not be configured independently in this example.

Step 8 Save the data.

```
huawei(config)#save
```

----End

12.4.2.9 Configuring the BTV Service

The OLT is connected to the remote gateway ONU through a GPON port to provide users with the bridge WAN multicast service.

Prerequisites

- The IPTV WAN ports on the ONU use factory defaults.
- The OLT has been connected to the BRAS and the multicast source.
- The ONU has been added to the OLT. For details, see **12.3.3 Adding an ONU to an OLT**.

Data Plan

Table 12-45 Data plan

Item	Data
ONU line profile	Profile name: ftto_line T-CONT ID: 4 GEM port ID: 13
ONU service profile	Profile name: ftto_ser ONU port capability set: adaptive
Traffic profile	ID: 8 802.1p priority: 4 CIR: off (unlimited) Priority-based scheduling policy: local-setting
Multicast service data	Multicast protocol: IGMP proxy Multicast version: IGMPv2 Multicast program: dynamic obtaining mode

Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Configure the OLT.

1. Configure a traffic profile.

   Configure traffic profile 8. Set the CIR to off (unlimited), priority to 4, and priority-based scheduling policy to local-setting (that is, queues are scheduled based on the priority specified in the profile).

   NOTE

   Run the **display traffic table ip** command to query existing traffic profiles in the system. If the existing traffic profiles in the system do not meet the requirements, run the **traffic table ip** command to add a traffic profile.

   ```
   huawei(config)#traffic table ip index 8 cir off priority 4 priority-policy local-setting
   ```

2. Configure the VLAN and service flows.

   Table 12-46 Data plan

VLAN Plan	VLAN Translation Policy
Single VLAN tag ● S-VLAN ID: 1000 ● MVLAN ID: 1000 ● VLAN type: smart ● VLAN attribute: common	ONU: duplicates multicast packets based on user ports and MVLANs are stripped off downstream. OLT: duplicates multicast packets based on PON ports with MVLAN unchanged.

   Configure the mapping between a GEM port and an Ethernet port on an ONU. If the ONU is connected to the STB through Ethernet port 2, map the service flow of Ethernet port 2 to GEM port 13 in the ONU line profile.

   ```
   huawei(config)#ont-lineprofile gpon profile-name ftto_line
   huawei(config-gpon-lineprofile-1)#gem mapping 13 2 vlan 1000
   huawei(config-gpon-lineprofile-1)#commit
   huawei(config-gpon-lineprofile-1)#quit
   ```

   Configure the multicast forwarding mode is untagged.

   ```
   huawei(config)#ont-srvprofile gpon profile-name ftto_ser
   huawei(config-gpon-srvprofile-1)#multicast-forward untag
   huawei(config-gpon-srvprofile-1)#commit
   huawei(config-gpon-srvprofile-1)#quit
   ```

   Create a service VLAN and add an upstream port to it. Add upstream port 0/19/0 to VLAN 1000.

   ```
   huawei(config)#vlan 1000 smart
   huawei(config)#port vlan 1000 0/19 0
   ```

   Create service flows. Set the service VLAN to 1000, GEM port ID to 13, and user VLAN to 1000, and use traffic profile 8.

   ```
   huawei(config)#service-port 1 vlan 1000 gpon 0/1/0 ont 1 gemport 13 multi-service
    user-vlan 1000 rx-cttr 8 tx-cttr 8
   ```


Copyright © Huawei Technologies Co., Ltd.

```
huawei(config)#service-port 2 vlan 1000 gpon 0/1/0 ont 2 gemport 13 multi-
service
 user-vlan 1000 rx-cttr 8 tx-cttr 8
```

3. Create an MVLAN and configure the IGMP version.

   Set the IGMP version for the MVLAN to IGMPv2.

```
huawei(config)#multicast-vlan 1000
huawei(config-mvlan1000)#igmp version v2
  This operation will delete all IPv4 programs with source IP addresses in the
current multicast VLAN
  Are you sure to change current IGMP version? (y/n)[n]:y
  Command is being executed. Please wait...
  Command has been executed successfully
```

4. Configure a program library.

   Set the mode for obtaining multicast programs to dynamic.

   NOTE

   You can set the mode for obtaining multicast programs to dynamic only when the IGMP mode is off.

```
huawei(config-mvlan1000)#igmp mode off
  Are you sure to close IGMP? (y/n)[n]:y
  Command is being executed. Please wait...
  Command has been executed successfully

huawei(config-mvlan1000)#igmp match mode disable
  Command has been executed successfully
```

   (Optional) Set the address range for the dynamic programs. If you need to limit the address range of dynamic programs, perform this operation. For example, set the address range of dynamic programs to 224.1.1.1-224.1.1.100.

```
huawei(config-mvlan1000)#igmp match group ip 224.1.1.1 to-ip 224.1.1.100
```

5. Set the IGMP mode.

   Select the IGMP proxy mode.

```
huawei(config-mvlan1000)#igmp mode proxy
  Are you sure to change IGMP mode? (y/n)[n]:y
  Command is being executed. Please wait...
  Command has been executed successfully
```

6. Configure the IGMP upstream port.

   Set the IGMP upstream port ID to 0/19/0 and working mode to **default**. Protocol packets are transmitted to all the IGMP upstream ports in the multicast VLAN.

```
huawei(config-mvlan1000)#igmp uplink-port 0/19/0
huawei(config-mvlan1000)#btv
huawei(config-btv)#igmp uplink-port-mode default
Are you sure to change the uplink port mode?(y/n)[n]:y
```

7. (Optional) Set multicast global parameters.

   In this example, the default settings are used for all the multicast global parameters.

8. Configure multicast users.

   Add service ports 1 and 2 as multicast users.

```
huawei(config-btv)#igmp user add service-port 1
huawei(config-btv)#igmp user add service-port 2
huawei(config-btv)#multicast-vlan 1000
huawei(config-mvlan1000)#igmp multicast-vlan member service-port 1
huawei(config-mvlan1000)#igmp multicast-vlan member service-port 2
huawei(config-mvlan1000)#quit
```

9. Save the data.

Copyright © Huawei Technologies Co., Ltd.

```
huawei(config)#save
```

Step 2 The ONU does not need to be configured.

----End

12.4.2.10 Configuring the VoD Service

The OLT is connected to the remote gateway ONU through a GPON port to provide users with the VoD service.

Prerequisites

- The IPTV WAN ports on the ONU use factory defaults.
- The OLT has been connected to the BRAS and the program source.
- The ONU has been added to the OLT. For details, see **12.3.3 Adding an ONU to an OLT**.

Data Plan

Table 12-47 Data plan

Item	Data
ONU line profile	Profile name: ftto_line T-CONT ID: 4 GEM port ID: 13
ONU service profile	Profile name: ftto_ser ONU port capability set: adaptive
Traffic profile	ID: 8 802.1p priority: 4 CIR: off (unlimited) Priority-based scheduling policy: local-setting

Procedure

Step 1 Configure the OLT.

1. Configure a traffic profile.

   Configure traffic profile 8. Set the CIR to off (unlimited), priority to 4, and priority-based scheduling policy to local-setting (that is, queues are scheduled based on the priority specified in the profile).

   NOTE

   Run the **display traffic table ip** command to query existing traffic profiles in the system. If the existing traffic profiles in the system do not meet the requirements, run the **traffic table ip** command to add a traffic profile.

Copyright © Huawei Technologies Co., Ltd.

```
huawei(config)#traffic table ip index 8 cir off priority 4 priority-policy
local-setting
```

2. Configure the VLAN and service flows.

Table 12-48 Data plan

VLAN Plan	VLAN Translation Policy
Single VLAN tag ● S-VLAN ID: 1100 ● VLAN type: smart ● VLAN attribute: common ● C-VLAN: 2001	The ONU adds CVALN tags to packets: untagged <-> C-VLAN tag. The OLT implements VLAN translation: C-VLAN tag <-> S-VLAN tag.

Configure the mapping between a GEM port and a VLAN. The service flow of user VLAN 2001 is mapped to GEM port 13 in the ONU line profile.

```
huawei(config)#ont-lineprofile gpon profile-name ftto_line
huawei(config-gpon-lineprofile-1)#gem mapping 13 4 vlan 2001
huawei(config-gpon-lineprofile-1)#commit
huawei(config-gpon-lineprofile-1)#quit
```

Create a service VLAN and add an upstream port to it. Add upstream port 0/19/0 to VLAN 1100.

```
huawei(config)#vlan 1100 smart
huawei(config)#port vlan 1100 0/19 0
```

Create service flows. Set the S-VLAN to 1100, GEM port ID to 13, and C-VLAN to 2001, and use traffic profile 8. Set the VLAN translation policy to Translate. The C-VLAN 2001 of the ONU is translated to S-VLAN 1100.

```
huawei(config)#service-port 3 vlan 1100 gpon 0/1/0 ont 1 gemport 13
multi-service user-vlan 2001 tag-transform translate rx-cttr 8 tx-cttr 8
huawei(config)#service-port 4 vlan 1100 gpon 0/1/0 ont 2 gemport 13
multi-service user-vlan 2001 tag-transform translate rx-cttr 8 tx-cttr 8
```

3. Save the data.

```
huawei(config)#save
```

Step 2 The ONU does not need to be configured.

----End

12.4.2.11 Configuring Link Aggregation, Congestion Control, and Security Policy

Service reliability is improved by configuring uplink aggregation and priority scheduling policy for queues in global configuration mode, and service security is improved by configuring security policy in global configuration mode.

Context

In link aggregation, multiple uplink Ethernet ports are aggregated into a group to increase bandwidth and reliability of uplinks of the OLT. You are advised to configure link aggregation.

Copyright © Huawei Technologies Co., Ltd.

Congestion control queues packets from one port into multiple queues and schedules the packets based on queue priorities. You are advised to configure congestion control.

Security policy involves system security, user security, and service security, ensuring service security from different aspects.

NOTE

- You are advised to enable the service security feature according to service types. For details, see **12.2.6 Principle of Security Data Plan**.
- The configuration of the system security, user security, and service security introduced in this topic is on the OLT side. The configuration on the ONU side is through the web and is simple, here we do not introduced it.

Procedure

- Configure link aggregation.

  On the OLT side, configure upstream ports 0/19/0 and 0/19/1 as an aggregation group. Each member port in the aggregation group is allocated packets based on the source MAC address. The working mode is LACP static aggregation.

  ```
  huawei(config)#link-aggregation 0/19 0-1 ingress workmode lacp-static
  ```

- Configure queue scheduling(On the OLT side).

  According to "**12.2.2 Principle of QoS Planning**", all packets are scheduled in strict priority queue mode and mapped into different queues based on priorities.

  ```
  huawei(config)#queue-scheduler strict-priority
  huawei(config)#cos-queue-map cos0 0 cos4 4 cos5 5 cos6 6
  ```

- Configure system security.
  - Enable deny of service (DoS) anti-attack on the OLT.
    1. Run the **security anti-dos enable** command to globally enable DoS anti-attack.
    2. Run the **security anti-dos control-packet policy** command to configure a protocol packet processing policy that will be used when a DoS attack occurs.
    3. Run the **security anti-dos control-packet rate** command to configure the threshold for the rate of sending protocol packets to the CPU.
  - Enable IP address anti-attack on the OLT.

    Run the **security anti-ipattack enable** command to enable IP address anti-attack.
- Configure user security.
  - Enable MAC address anti-flapping on the OLT.

    Run the **security anti-macduplicate enable** command to enable MAC address anti-flapping.
  - Enable MAC address anti-spoofing on the OLT.
    1. In global config mode, run the **security anti-macspoofing enable** command to globally enable MAC address anti-spoofing.
    2. Enable MAC address anti-spoofing at VLAN level in global config mode or service profile mode:
       a. In global config mode, run the **security anti-macspoofing vlan** command to enable MAC address anti-spoofing.
       b. Perform the following operations to enable MAC address anti-spoofing in service profile mode:

Copyright © Huawei Technologies Co., Ltd.

a. In global config mode, run the **vlan service-profile** command to create a VLAN service profile.
b. Run the **security anti-macspoofing enable** command to enable MAC address anti-spoofing at VLAN level.
c. Run the **commit** command to make the profile configuration take effect.
d. Run the **quit** command to quit the VLAN service profile mode.
e. Run the **vlan bind service-profile** command to bind the created VLAN service profile to a VLAN.

3. (Optional) Run the **security anti-macspoofing max-mac-count** command to set the maximum number of MAC addresses that can be bound to a service flow.
4. (Optional) Run the **security anti-macspoofing exclude** command to configure the types of packets for which MAC address anti-spoofing does not take effect, such as Internet Group Management Protocol (IGMP) packets.

- Configure service security.
  - Enable Dynamic Host Configuration Protocol (DHCP) Option 82 on the OLT. This configuration is recommended for the DHCP-based Internet access service.
    1. DHCP Option 82 can be enabled or disabled at four levels: global, port, VLAN, and service port levels. This function takes effect only after it is enabled at the four levels. Among the four levels, DHCP Option 82 is disabled only at the global level by default.
       - The global level: In global config mode, run the **dhcp option82** command to enable DHCP Option 82 at the global level.

         When you run this command, select the **enable**, **forward**, or **rebuild** parameter based on site requirements. The three parameters can all enable DHCP Option 82 but provide different packet processing policies on the OLT. For details, see the **dhcp option82** command.
       - The port level: In global config mode, run the **dhcp option82 port** or **dhcp option82 board** command to enable DHCP Option 82 at the port level.
       - The VLAN level:
         a. In global config mode, run the **vlan service-profile** command to create a VLAN service profile.
         b. Run the **dhcp option82 enable** command to enable DHCP Option 82 at the VLAN level.
         c. Run the **commit** command to make the profile configuration take effect.
         d. Run the **quit** command to quit the VLAN service profile mode.
         e. Run the **vlan bind service-profile** command to bind the created VLAN service profile to a VLAN.
       - The service port level: In global config mode, run the **dhcp option82 service-port** command to enable DHCP Option 82 at the service port level.
    2. On the OLT, run the **dhcp-option82 permit-forwarding service-port** command with the **enable** parameter selected, to allow ONU DHCP packets to carry Option 82 information.
  - Enable Policy Information Transfer Protocol (PITP) on the OLT. This configuration is recommended for the PPPoE-based Internet access service.

Copyright © Huawei Technologies Co., Ltd.

1. PITP can be enabled or disabled at four levels: global, port, VLAN, and service port levels. This function takes effect only after it is enabled at the four levels. Among the four levels, PITP is disabled only at the global level by default.
   - The global level: In global config mode, run the **pitp enable pmode**, **pitp forward pmode**, or **pitp rebuild pmode** command to enable PITP at the global level.

     In the preceding commands, the **enable**, **forward**, and **rebuild** parameters can all enable PITP but provide different packet processing policies on the OLT. Select one of them based on site requirements. For details, see the **pitp** command.
   - The port level: In global config mode, run the **pitp port** or **pitp board** command to enable PITP at the port level.
   - The VLAN level:
     a. In global config mode, run the **vlan service-profile** command to create a VLAN service profile.
     b. Run the **pitp enable** command to enable PITP at the VLAN level.
     c. Run the **commit** command to make the profile configuration take effect.
     d. Run the **quit** command to quit the VLAN service profile mode.
     e. Run the **vlan bind service-profile** command to bind the created VLAN service profile to a VLAN.
   - The service port level: In global config mode, run the **pitp service-port** command to enable PITP at the service port level.
2. On the OLT, run the **pitp permit-forwarding service-port** command with the **enable** parameter selected, to allow ONU PPPoE packets to carry a vendor tag.

----End

12.4.2.12 Verifying Services

In the FTTO scenario, ONUs are installed at users' houses or in business buildings which are far away from the central equipment room. ONUs provide remote service verification methods including PPPoE dialup emulation, call emulation, and multicast emulation to facilitate configuration and commissioning engineers to verify services remotely after service configuration.

Prerequisites

ONUs and upper-layer devices have been connected properly. The BRAS and MGC/IMS have been configured.

Copyright © Huawei Technologies Co., Ltd.

Background

Remote Service Verification Method	Function	Description
PPPoE dialup emulation	An ONU simulates a PPPoE user terminal software to perform dialup and interact with the BRAS to verify the connectivity between the ONU and BRAS.	● PPPoE dialup emulation requires a service flow which does not belong to a QinQ VLAN. ● A user name, password, and authentication mode must be configured on the BRAS for the PPPoE dialup emulation. ● An ONU supports a maximum of a PPPoE dialup emulation.
Call Emulation	An ONU simulates a voice user to make a call to check whether the voice service data is correctly configured. You can also use the call emulation function to locate a fault when the voice service is faulty.	● An ONU can simulate a caller or callee to communicate with a phone in a call. In this case, only a functional phone is required in the central office where the acceptance personnel locate. ● An ONU supports only once call emulation.
Multicast emulation	This function enables you to simulate a multicast user going online and lead the program stream to an ONU. You can check whether the multicast service is normal by checking the real-time traffic of the multicast program.	Multicast services configured in the dynamic controllable multicast mode do not support this function.

Data plan

Item	Data	Remarks
PPPoE dialup emulation parameters	PPPoE user name: test@huawei Password: test	The user name, password, and authentication mode for the emulation test must be configured on the BRAS. The entered user name, password, and authentication mode must be consistent with those configured on the BRAS.
Call emulation parameters	ONU POTS ID: 1	The default values are used. You can run the **display pots emulational configuration** command to check the parameter values.

Copyright © Huawei Technologies Co., Ltd.

Item	Data	Remarks
Multicast emulation parameters	Multicast service flow ID: 1 MVLAN: 1000 IP address of the multicast program: 224.1.1.10	-

Procedure

- Verify the Internet access service using PPPoE dialup emulation.
  1. In the xPON board mode, run the **pppoe simulate start** command to start a PPPoE dialup emulation test.

     The service is functional if the test result is **success**. The following test uses GPON as an example:

```
huawei(config)#interface gpon 0/1
huawei(config-if-gpon-0/1)#pppoe simulate start
{ portid<U><0,7> }:0
{ ontid<U><0,127> }:1
{ eth<K>|untagged<K>|vlanid<U><0,4095> }:eth
{ ont-portid<U><1,8> }:4
{ untagged<K>|vlanid<U><0,4095> }:100
{ priority<U><0,7>|user-name<K> }:user-name
{ username<S><Length 1-64> }:test@huawei
{ user-password<K> }:user-password
{ password<S><Length 1-64> }:test
{ authentication-mode<K> }:authentication-mode
{ protocol<E><chap,pap> }:chap

  Command:
          pppoe simulate start 0 1 eth 4 100 user-name test@huawei user-
password
 test authentication-mode chap

huawei(config-if-gpon-0/1)#
  ---------------------------------
  ONT PPPoE Test Result
  ---------------------------------
  F/S/P                : 0/1/0
  ONT-ID               : 1
  ONT ETH Port ID      : 4
  ONT Vlan ID          : 100
  Vlan Priority        : -
  Emluator result      : Success
  Session ID           : 18814
  User IP              : 172.16.100.109
  Gateway IP           : 172.16.100.1
  ---------------------------------
```

- Troubleshooting methods for the Internet access service
  1. Check whether configurations are complete on the OLT.
     - Run the **display ont info** command to query the ONU status to check whether the ONU is registered successfully.
     - Run the **display service-port** command to check whether the Internet access service flow is configured and whether the inner VLAN ID of the service flow is consistent with that in the data plan.

Copyright © Huawei Technologies Co., Ltd.

- If a native VLAN is configured for the Ethernet port on the ONU, run the **display ont port attribute** command in the xPON board mode to check whether the native VLAN is correct.

2. Check the upstream and downstream ports by checking the MAC address learning status.
   a. Run the **display mac-address vlan** command to check the MAC address learning status of the Internet service VLAN.
      - If the upstream port does not learn a MAC address, check the network connections between the upstream port and upper-layer devices and check the configurations of upper-layer devices.
      - If the downstream port does not learn a MAC address, check whether the ONU is activated, whether the PC is connected to the right port on the ONU, and whether the PC is working properly.
   b. Run the **display ont-learned-mac** command to check whether the ONU connecting to the PON port learned any MAC addresses.

      If not, check whether the ONU properly connects to the PC or home gateway (HGW).

- Verify the voice service using call emulation.
  1. Run the **ont emulational call** command to configure a call emulation test.

```
huawei(config)#test
huawei(config-test)#ont emulational call caller-port 0/1/0 1 1 telno
28777192
{ <cr>|caller-stop-time<K> }:

  Command:
          ont emulational call caller-port 0/1/0 1 1 telno 28777192
```

  2. The ONU outputs the call emulation result after the test is complete.

     The service is functional if the test result is **success**.

```
huawei(config-test)#
  ------------------------------------------------------------------
  F/S/P                : 0/1/0
  ONT-ID               : 0
  ONT-POTSID           : 1
  Test type            : caller emulational call test
  Detected number      : 28777192
  Reported number      : 28777192
  Current status       : test end
  Test Result          : success
  ------------------------------------------------------------------
```

- Troubleshooting methods for the voice service.
  1. Check whether configurations are complete on the OLT.
     - Run the **display ont info** command to query the ONU status to check whether the ONU is registered successfully.
     - Run the **display service-port** command to check whether the voice service flow is configured and whether the inner VLAN ID of the service flow is consistent with that in the data plan.
  2. Check the upstream and downstream ports by checking the MAC address learning status.

     Run the **display mac-address vlan** command to check the MAC address learning status of the voice service VLAN.

Copyright © Huawei Technologies Co., Ltd.

- If the upstream port does not learn a MAC address, check the network connections between the upstream port and upper-layer devices and check the configurations of upper-layer devices.
- If the downstream port does not learn a MAC address, check whether the ONU is activated and whether physical links are normal.
- If both the upstream and downstream ports can learn the MAC address, record the MAC address of the ONU and log in to the service router (SR) to check whether an IP address is allocated to the MAC address.

3. Check the registration status of the voice service.
   - You can run the **display ont port state** command on the OLT to query the call connection status on the POTS port. If **Call State** is **RegisterFail** or **Connecting** for a long time, check whether the voice configuration on the MGC/SIP server is consistent with that on the ONU.
   - If the ONU uses the H.248 protocol, you can run the **display ont mg status** command on the OLT to query the registration status of the MG interface that connects to the ONU. If **MG Status** is **UnRegistered** or **Registering** for a long time, check whether the voice configuration on the MGC/SIP server is consistent with that on the ONU.
   - You can query the registration status of the voice service on the ONU web page. If the query result shows that the registration fails or the voice service is in the registering state for a long time, check whether the voice configuration on the MGC/SIP server is consistent with that on the ONU.

- Verify the multicast service using multicast emulation.
  1. Run the **igmp static-join** command to simulate a multicast user to order a multicast program.

     ```
     huawei(config)#btv
     huawei(config-btv)#igmp static-join service-port 1 ip 224.1.1.10 vlan 1000
     ```

     NOTE

     If the multicast program is obtained dynamically, **igmp static-join** can be executed successfully only when the range for obtaining the dynamic program is set.

  2. Run the **display igmp user** command to query the status of the multicast user.

     The multicast user is normal if the queried result is **online**.

     ```
     huawei(config-btv)#display igmp user service-port 1
       User                       : 0/1/0/1
       State                      : online
       Authentication             : no-auth
       Quick leave                : MAC-based
       IGMP flow ID               : 1
       Video flow ID              : 1
       Log switch                 : enable
       Bind profiles              : -
       IGMP version               : IGMP v3
       Current version            : IGMP v3
       Current IGMP IPv6 version  : IGMP IPv6 v2
       Available programs         : 8
       Global leave               : disable
       User max bandwidth         : no-limit
       Used bandwidth(kbps)       : 0
       Used bandwidth
       to max bandwidth(%)        : -
       Total video bandwidth      : -
       Mcast video bandwidth      : -
       Active program list
     ```


Copyright © Huawei Technologies Co., Ltd.

```
------------------------------------------------------------------------
--
  Program name     VLAN  IP/MAC          State          Start time

------------------------------------------------------------------------
--
  PROGRAM-5        1000  224.1.1.10      watching       2011-10-29
                                                       16:33:41+08:00

------------------------------------------------------------------------
--
  Total: 1
```

3. Run the **display multicast flow-statistic** command to query the real-time traffic of the multicast program.

   The multicast program can be ordered if the queried result is a non-empty value.

```
huawei(config-btv)#display multicast flow-statistic vlan 1000 ip
224.1.1.10
{ <cr>|sourceip<K> }:

  Command:
          display multicast flow-statistic vlan 1000 ip 224.1.1.10
  Command is being executed. Please wait...
  Multicast flow statistic result: 8736(kbps)
```

----End

12.4.3 Layer 2 Interoperation Service Between Enterprise Branches

Different branches of an enterprise can achieve Layer 2 interoperation through ONUs. Then, different branches can transmit service traffic to each other just like in the same LAN, which can improve coordination work efficiency.

12.4.3.1 Service Requirement and Application Scenario

Service Requirement

An enterprise that has multiple branches requires intercommunication between different branches or between its headquarter and branches. Virtual private network (VPN) can achieve secure interconnection but requires additional devices and complex management. It requires high costs even if a leased VPN is used. In addition, the bandwidth provided by a VPN is limited due to restricted VPN access modes and the bandwidth control is inflexible.

To address the preceding problems, the Layer 2 interoperation technology using fiber access is put forward and becomes the main trend.

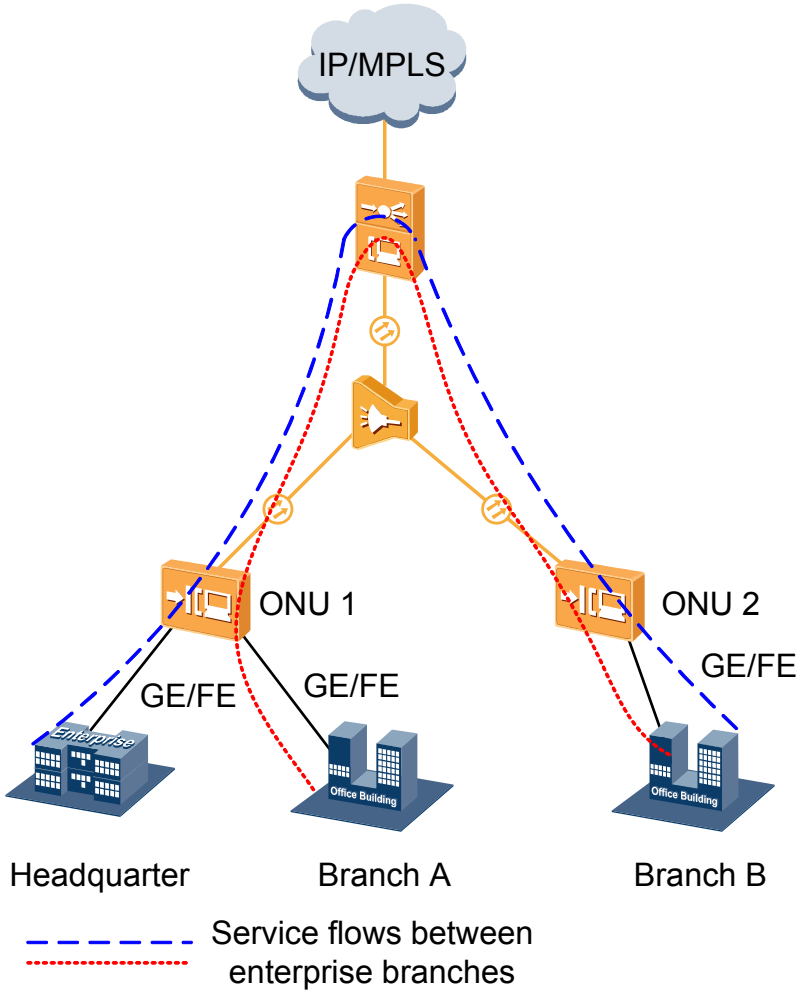
Application Scenario

As shown in **Figure 12-13**, ONUs are deployed in branches of an enterprise. The ONUs access and converge Ethernet services of the enterprise through GE/FE ports and transmit the services to the OLT. The OLT implements Layer 2 interoperation between different branches of the enterprise.

ONUs supporting this scenario: MA5612, MA5628, MA5616

Copyright © Huawei Technologies Co., Ltd.

Figure 12-13 Network diagram for Layer 2 interoperation between enterprise branches



Note: Because the bandwidth of upstream and downstream PON ports is fixed, the number of enterprises connected to an OLT is limited when the enterprises require symmetric bandwidth. When an enterprise requires 100 Mbit/s symmetric bandwidth and uses an 8-channel PON board:

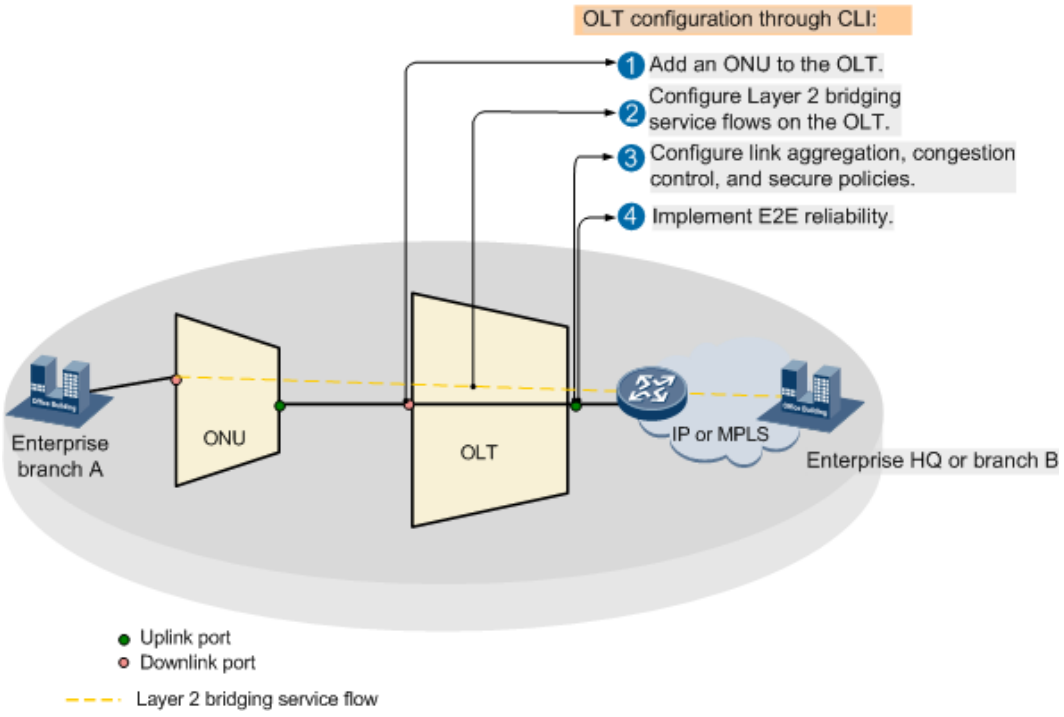
1. The number of enterprises or branches connected to a PON port should not exceed eight.
2. The number of enterprises or branches connected to a PON board should not exceed 64.
3. The number of enterprises connected to an OLT cannot exceed 200 (20G/100M) if the upstream bandwidth is 2 x 10GE. (The number of enterprises connected to an OLT is mainly restricted by the upstream bandwidth.)

12.4.3.2 Configuration Procedure

Figure 12-14 shows the configuration procedure for Layer 2 interoperation between branches of an enterprise.

Copyright © Huawei Technologies Co., Ltd.

Figure 12-14 Configuration procedure for Layer 2 interoperation between branches of an enterprise



The following table lists the detailed description steps.

Item	Procedure	Remarks
OLT	**Adding an ONU to an OLT**	This topic describes how to add ONUs to the OLT. ONUs can be configured only after they are added to the OLT successfully.
OLT	**Configuring Layer 2 Interoperation Service Ports on OLT**	None
OLT	**Configuring Congestion Control and Security Policies**	This topic describes how to configure global priority-based scheduling policies for upstream queues to ensure service reliability and configure global security policies to ensure service security.
OLT	**Configuring E2E Reliability**	The upstream and downstream networking protection ensures the E2E reliability. Link aggregation and protection groups can be configured for upstream networking protection. Type x protection for PON ports can be configured for downstream networking protection.
OLT	**Verifying Services**	None

Copyright © Huawei Technologies Co., Ltd.

12.4.3.3 Adding ONUs to OLT

This topic describes how to add ONUs to the OLT. ONUs can be configured only after they are added to the OLT successfully.

Context

- When adding ONUs, you need to bind related profiles to the ONUs, including the DBA profile, line profile, service profile, and alarm profile. For the functions of each profile and how to configure profiles, see **Table 12-49**.

Table 12-49 ONU profile

Profile Type	Function	Command
DBA profile	Describes GPON traffic parameters. A T-CONT is bound to a DBA profile for dynamic bandwidth allocation, improving upstream bandwidth utilization.	Query: **display dba-profile** Add: **dba-profile add**
Line profile	Describes the binding relationship between T-CONTs and DBA profiles, QoS mode of service flows, and mapping between GEM ports and services on ONUs.	Query: **display ont-lineprofile** Add: **ont-lineprofile add**
Service profile	Describes the parameters of the ONT managed by the OLT in OMCI mode.	Query: **display ont-srvprofile** Add: **ont-srvprofile add**
Alarm profile	Provides a series of alarm threshold parameters that are used for performance measurement and monitoring of activated ONU lines.	Query: **display gpon alarm-profile** Add: **gpon alarm-profile add**

- An ONU can be added in two modes. Select either mode as required.

Mode	Usage Scenario	Command
Offline addition	The password or serial number of an ONU has been obtained.	Run the **ont add** command to add the ONU.
Online confirmation	The password and serial number of an ONU are unknown.	Run the **port ont-auto-find** command in the GPON mode to enable the automatic discovery function for the GPON port and run the **ont confirm** command to add the ONU.

Copyright © Huawei Technologies Co., Ltd.

Data Planning

Table 12-50 Key data plan

Configuration Item	Data
DBA profile	Profile ID: 20 Profile type: Type 3 Assured bandwidth: 100 Mbit/s Maximum bandwidth: 120 Mbit/s
Line profile	Profile ID: 10 T-CONT ID: 4 GEM port ID for Layer 2 interoperation service: 12
Service profile	Profile ID: 11 Ethernet and POTS port capability set: adaptive ID of the ONU Ethernet VLAN: 300 **NOTE** Ensure that the capability set of the service profile is greater than or equal to that of the device. Otherwise, some ports fail to be configured.
Networking data	For example, add two ONUs (ONU 1 and ONU 2) for carrying services of different branches. ● ONU 1 is connected to PON port 0/3/1. ● ONU 2 is connected to PON port 0/4/1.

Procedure

Step 1 Configure GPON ONU profiles.

1. Configure a DBA profile.

   ```
   huawei(config)#dba-profile add profile-id 20 type3 assure 102400 max 122880
   ```

2. Configure an ONU line profile.

   a. Create GPON ONU line profile 10.

   ```
   huawei(config)#ont-lineprofile gpon profile-id 10
   ```

   NOTE

   Create a line profile according to the data plan. The ID of the line profile to be created cannot conflict with existing profile IDs in the system. In this example, the ID of the line profile is 10.

   b. In the line profile configuration mode, bind T-CONT 4 to DBA profile 20.

   ```
   huawei(config-gpon-lineprofile-10)#tcont 4 dba-profile-id 20
   ```

   c. In the line profile configuration mode, bind GEM ports to T-CONTs.

   Add GEM port 12 for carrying the Layer 2 interoperation service flow.

Copyright © Huawei Technologies Co., Ltd.

GEM port 11 is bound to T-CONT 4. During configuration, set QoS policies for each service flow. For details on QoS data planning, see **13.2.3 Principle of QoS Data Plan**.

```
huawei(config-gpon-lineprofile-10)#gem add 12 eth tcont 4 cascade on
```

d. Configure mapping between GEM ports and ONU-side services.

Set the mapping mode to VLAN mode (the default mode). Map Layer 2 interoperation service flow (C-VLAN 300) to GEM port 12.

```
huawei(config-gpon-lineprofile-10)#gem mapping 12 1 vlan 300
```

e. After the configuration is complete, run the **commit** command to make the configured parameters take effect.

```
huawei(config-gpon-lineprofile-10)#commit
huawei(config-gpon-lineprofile-10)#quit
```

3. Configure an ONU service profile.

a. Create a GPON ONU service profile with ID 11.

```
huawei(config)#ont-srvprofile gpon profile-id 11
```

NOTE

Ensure that the ID of the service profile to be created does not exist in the system. Create a service profile according to the planned data. Service profile 11 is used as an example.

b. Configure the Ethernet and POTS port capability set to **adaptive**. Then, the system adapts the capability to the actual capability of the online ONU.

```
huawei(config-gpon-srvprofile-11)#ont-port eth adaptive pots adaptive
```

c. Add Ethernet port 1 to VLAN 300.

```
huawei(config-gpon-srvprofile-11)#port vlan eth 1 300
```

d. Run the **commit** command to make the configurations take effect.

```
huawei(config-gpon-srvprofile-11)#commit
huawei(config-gpon-srvprofile-11)#quit
```

4. Set the ID of the native VLAN containing Ethernet port 1 to 300.

```
huawei(config)#interface gpon 0/3
huawei(config-if-gpon-0/3)#ont port native-vlan 1 1 eth 1 vlan 300
huawei(config-if-gpon-0/3)#quit
huawei(config)#interface gpon 0/4
huawei(config-if-gpon-0/4)#ont port native-vlan 1 2 eth 1 vlan 300
huawei(config-if-gpon-0/4)#quit
```

5. (Optional) Configure an alarm profile.

- The default GPON alarm profile ID is 1. The value of each alarm threshold is **0** which indicates that alarms are not reported.
- In this example, the default alarm profile is used and no configuration is required.

Step 2 Add ONUs to the OLT.

1. Add ONU 1 and ONU2 in offline mode.

Connect ONU 1 and ONU 2 to GPON ports 0/3/1 and 0/4/1 respectively through an optical splitter. The serial numbers of the two ONUs are 32303131B39FD641 and 32303131B39FD642 respectively, and the management mode is OMCI. Both the ONUs are bound to line profile 10 and service profile 11.

```
huawei(config)#interface gpon 0/3
huawei(config-if-gpon-0/3)#ont add 1 ontid 1 sn-auth 32303131B39FD641
omci ont-lineprofile-id 10 ont-srvprofile-id 11
huawei(config-if-gpon-0/3)#quit
```


Copyright © Huawei Technologies Co., Ltd.

```
huawei(config)#interface gpon 0/4
huawei(config-if-gpon-0/4)#ont add 1 ontid 2 sn-auth 32303131B39FD642
omci ont-lineprofile-id 10 ont-srvprofile-id 11
```

2. (Optional) Bind an alarm profile.

   By default, an ONU will be automatically bound to alarm profile 1 (default profile). You need to manually bind an alarm profile to an ONU only when the default alarm profile does not meet requirements.

   In this example, the default alarm profile is used. Therefore, you do not need to manually bind an alarm profile.

Step 3 Confirm the ONU status.

After adding an ONU, run the **display ont info** command to query the current status of the ONU. Ensure that **Control flag** is **active**, **Run State** is **online**, and **Config state** is **normal**.

The following uses ONU 1 as an example to describe how to confirm ONU status.

```
huawei(config-if-gpon-0/3)#display ont info 1 1
  ------------------------------------------------------------------------
  F/S/P                : 0/3/1
  ONT-ID               : 1
  Control flag         : active    //Indicates that the ONU is
activated.
  Run state            : online    //Indicates that the ONU is
online.
  Config state         : normal    //Indicates that the ONU is in normal
state.
...//Other command output is omitted.
huawei(config-if-gpon-0/3)#quit
```

----End

Follow-up Procedure

When **Config state** is **failed**, **Run state** is **offline**, or **Match state** is **mismatch**:

- If **Control flag** is **deactive**, run the **ont active** command in GPON mode to activate the ONU.
- If **Run state** is **offline**, a physical line may be broken or the optical module may be damaged. Check the line and the optical module.
- If **Config state** is **failed**, the configured ONU capability exceeds the actual ONU capability. In this case, run the **display ont failed-configuration** command in the diagnose mode to check the failed configuration item and the failure cause. Then, rectify the fault accordingly.
- If the ONU does not match, that is, **Match state** is **mismatch**, the port types and number of ports undermatch the actual port types and number of ports supported by the ONU. In this case, run the **display ont capability** command to query the actual capability of the ONU, and then select one of the following modes to modify the ONU configuration:
  - Create a proper ONU profile according to the actual capability of the ONU, and then run the **ont modify** command to modify the configuration data of the ONU.
  - Modify the ONU profile according to the actual capability of the ONU and save the modification. Then, the ONU automatically recovers the configuration successfully.

Copyright © Huawei Technologies Co., Ltd.

12.4.3.4 Configuring Layer 2 Interoperation Service Ports on OLT

This topic describes how to configure service ports on the OLT for Layer 2 interoperation so that data packets sent from different ONUs can be forwarded based on the same VLAN at Layer 2.

Prerequisites

1. The main control board on the device is an SCUN board.
2. The ARP proxy function is disabled using the **arp proxy disable** command. (The Layer 2 interoperation function and ARP proxy function are mutually exclusive.)

Data Plan

Configuration Item	Data
Layer 2 interoperation SVLAN	OLT VLAN ID (the OLT transparently transmits VLANs of ONU): 300 VLAN forwarding mode: vlan-mac (default) ONU VLAN ID: 300 Service flow ID: 301
Traffic profile	Profile ID: 10 Assured bandwidth: 100 Mbit/s Priority source: user-cos Default priority: 4

NOTE

For detailed data planning, see **13.2.2 Principle of VLAN Data Plan**.

Procedure

Step 1 Configure an SVLAN and add an upstream port to it.

Set the SVLAN ID of the Layer 2 interoperation service to 300, VLAN type to smart VLAN, and add upstream port 0/19/0 to the VLAN.

```
huawei(config)#vlan 300 smart
huawei(config)#port vlan 300 0/19 0
```

Step 2 Configure a traffic profile.

Add a new traffic profile 10 and set the assured rate to 100 Mbit/s. Packets transmitted upstream use the priority (4 by default) copied from the user side. Packets transmitted downstream use the priority carried by themselves.

```
huawei(config)#traffic table ip index 10 cir 102400 priority user-cos 4 priority-policy tag-in-package
```

Step 3 Configure a service port to receive and transparently transmit the Layer 2 interoperation service that is sent from ONU 1 and ONU 2.

Copyright © Huawei Technologies Co., Ltd.

Set the service attributes based on the data plan:

- For the OLT, set the SVLAN ID to 300, CVLAN ID to 300 which is the same as the upstream VLAN ID of the ONU, and GEM port ID to 12 for the Layer 2 interoperation service.
- For ONUs, set the upstream VLAN ID to 300.

```
huawei(config)#service-port 301 vlan 300 gpon 0/3/1 ont 1 gemport 12 multi-service
user-vlan 300 rx-cttr 10 tx-cttr 10
huawei(config)#service-port 302 vlan 300 gpon 0/4/1 ont 2 gemport 12 multi-service
user-vlan 300 rx-cttr 10 tx-cttr 10
```

Step 4 Configure attributes for protocol transparent transmission.

Create a VLAN service profile, enable the VLAN Layer 2 interoperation function, and configure attributes for protocol transparent transmission. Then, bind the profile to VLAN 300. For details on data planning for protocol transparent transmission, see **13.2.4 Principle of Protocol Transparent Transmission Data Plan**.

```
huawei(config)#vlan service-profile profile-id 1
huawei(config-vlan-srvprof-1)#user-bridging enable   //Mandatory
huawei(config-vlan-srvprof-1)#bpdu tunnel enable
huawei(config-vlan-srvprof-1)#ospf tunnel enable
huawei(config-vlan-srvprof-1)#rip tunnel enable
huawei(config-vlan-srvprof-1)#vtp-cdp tunnel enable
huawei(config-vlan-srvprof-1)#commit
huawei(config-vlan-srvprof-1)#quit
huawei(config)#multicast-unknown policy service-port 301 transparent
huawei(config)#multicast-unknown policy service-port 302 transparent
huawei(config)#vlan bind service-profile 300 profile-id 1
```

----End

12.4.3.5 Configuring Congestion Control and Security Policies

This topic describes how to configure global priority-based scheduling policies for upstream queues to ensure service reliability and configure global security policies to ensure service security.

Context

Congestion control uses queue scheduling technology to map packets sent from the same port into multiple queues and process packets in each queue based on priority. Congestion control is recommended.

Security policies cover system security, user security, and service security, which ensure normal running of services.

NOTE

- You are advised to enable the service security feature according to service types. For details, see **13.2.5 Principle of Security Data Plan**.
- The configuration of the system security, user security, and service security introduced in this topic is on the OLT side. The configuration on the ONU side is through the web and is simple, here we do not introduced it.

Procedure

- Configure queue scheduling.

Copyright © Huawei Technologies Co., Ltd.

Based on **13.2.3 Principle of QoS Data Plan**, all packets use strict priorities for queue scheduling and are mapped to queues based on priorities.

```
huawei(config)#queue-scheduler strict-priority
huawei(config)#cos-queue-map cos0 0 cos1 1 cos2 2 cos3 3 cos4 4 cos5 5 cos6 6 cos7 7  //System default
```

- Configure system security policies.
  - Enable deny of service (DoS) anti-attack on the OLT.
    1. Run the **security anti-dos enable** command to globally enable DoS anti-attack.
    2. Run the **security anti-dos control-packet policy** command to configure a protocol packet processing policy that will be used when a DoS attack occurs.
    3. Run the **security anti-dos control-packet rate** command to configure the threshold for the rate of sending protocol packets to the CPU.
  - Enable IP address anti-attack on the OLT.

    Run the **security anti-ipattack enable** command to enable IP address anti-attack.
- Configure user security policies.
  - Enable MAC address anti-flapping on the OLT.

    Run the **security anti-macduplicate enable** command to enable MAC address anti-flapping.
  - Enable IP address anti-spoofing on the OLT.
    1. In global config mode, run the **security anti-ipspoofing enable** command to globally enable IP address anti-spoofing.
    2. Enable IP address anti-spoofing at VLAN level, perform the following operations to enable IP address anti-spoofing in service profile mode:
       a. Run the **vlan service-profile** command to create a VLAN service profile.
       b. Run the **security anti-ipspoofing enable** command to enable IP address anti-spoofing at VLAN level.
       c. Run the **commit** command to make the profile configuration take effect.
       d. Run the **quit** command to quit the VLAN service profile mode.
       e. Run the **vlan bind service-profile** command to bind the created VLAN service profile to a VLAN.
  - The service port level: In global config mode, run the **security anti-ipspoofing service-port** *serviceport-id* **enable** command to enable IP address anti-spoofing at the service port level.

----End

12.4.3.6 Configuring E2E Reliability

This topic describes how to configure end-to-end (E2E) protection schemes for the enterprise private line service which has a high requirement on service reliability.

Context

Reliability covers equipment reliability, upstream networking protection, and downstream networking protection. For details on reliability data planning, see **13.2.6 Principle of Reliability Data Plan**.

Copyright © Huawei Technologies Co., Ltd.

- Upstream networking protection includes link aggregation group and protection group. Usually, link aggregation group is configured when the GIU board is used to transmit traffic upstream; protection group is configured when the main control board is used to transmit traffic upstream. The two protection schemes are not configured at the same time.
- Downstream networking protection includes Type B, Type C single homing, and Type C dual homing, which are used to protect service ports. Ports on the same ONU can be configured only with the same protection scheme.

NOTE

This topic describes how to configure five mainstream protection schemes. Select required protection schemes based on the carrier's requirement and actual networking scenario.

Procedure

- Configure a link aggregation group.

  Bind upstream ports 0/19/0 and 0/19/1 together as an aggregation link group. Each member port in the group transmits packets based on source MAC addresses. The working mode is LACP static aggregation.

  ```
  huawei(config)#link-aggregation 0/19 0-1 ingress workmode lacp-static
  ```

- Configure a protection group.

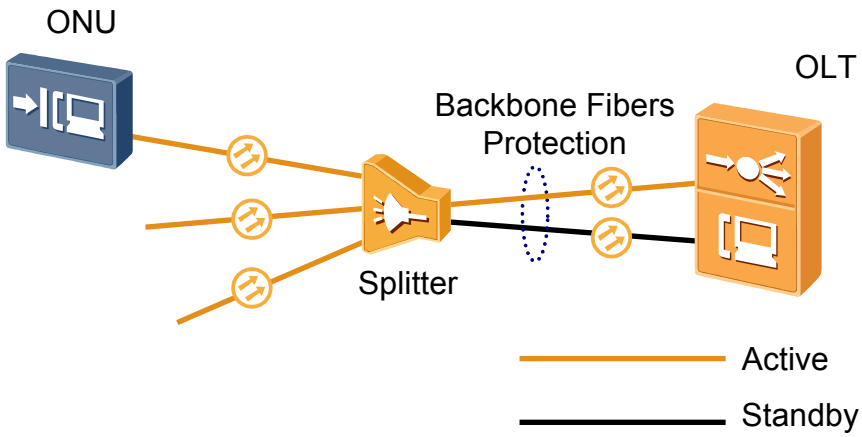
  Configure upstream ports 0/19/0 and 0/19/1 on board GIU as a port protection group. Set port 0/19/0 as the working port and port 0/19/1 as the protection port, set the working mode to time delay detection, and enable the protection group.

  ```
  huawei(config-protect)#protect-group first 0/19/0 second 0/19/1 eth workmode timedelay enable
  ```

- Configure the Type B protection.

  Figure 12-15 shows the Type B protection networking diagram.

  Figure 12-15 Type B protection

  Configure redundancy backup for ports 0/3/1 and 0/3/2 on the same GPON board on OLT. When port 0/3/1 fails, the system can automatically switch to port 0/3/2.

  ```
  huawei(config)#protect-group 0 protect-target gpon-uni-port workmode timedelay
  huawei(protect-group-0)#protect-group member port 0/3/1 role work
  huawei(protect-group-0)#protect-group member port 0/3/2 role protect
  huawei(protect-group-0)#protect-group enable
  ```


Copyright © Huawei Technologies Co., Ltd.

NOTE

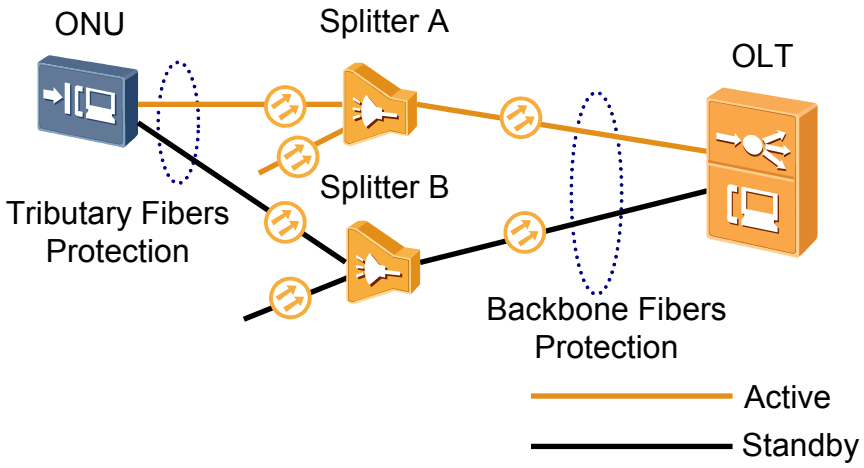
The configurations of services accessed by the ONUs remain the same after the Type B protection is configured. That is, the service configurations are applied only to the working GPON port.

- Configure the Type C single homing protection.

  Figure 12-16 shows networking diagram for the Type C single homing protection. Configure two 1:N optical splitters, one for connecting the working PON ports on the OLT and ONUs, and one for connecting the protection PON ports on the OLT and ONUs. This protection scheme protects both the backbone fibers and tributary fibers.

  The configurations of services accessed by the ONUs remain the same after the Type C single homing protection is configured. That is, the service configurations are applied only to the working PON port on the OLT and working upstream PON ports on the ONUs.

  Figure 12-16 Type C single homing protection



  As shown in the preceding figure, Type C single homing protecting is configured for optical fiber links between the OLT and ONU.

  - The ports on the GPON service board are 0/3/1 and 0/3/2.
  - The link at port 0/3/1 is the working link.
  - The link at port 0/3/2 is the protection link.
  - The ONU ID is 1.
  - The ONU is authenticated by serial number (SN). The SN of the ONU is 32303131B39FD641 and the management mode is SNMP.
  - The ID of the line profile bound to the ONU is 10.

```
huawei(config)#interface gpon 0/3
huawei(config-if-gpon-0/3)#ont add 1 1 sn-auth 32303131B39FD641 snmp ont-
lineprofile-id 10
huawei(config-if-gpon-0/3)#ont add 2 1 protect-side
huawei(config-if-gpon-0/3)#quit
huawei(config)#protect-group protect-target gpon-uni-ont workmode portstate
huawei(protect-group-1)#protect-group member port 0/3/1 ont 1 role work
huawei(protect-group-1)#protect-group member port 0/3/2 ont 1 role protect
huawei(protect-group-1)#protect-group enable
huawei(protect-group-1)#quit
```

- Configure the Type C dual homing protection.

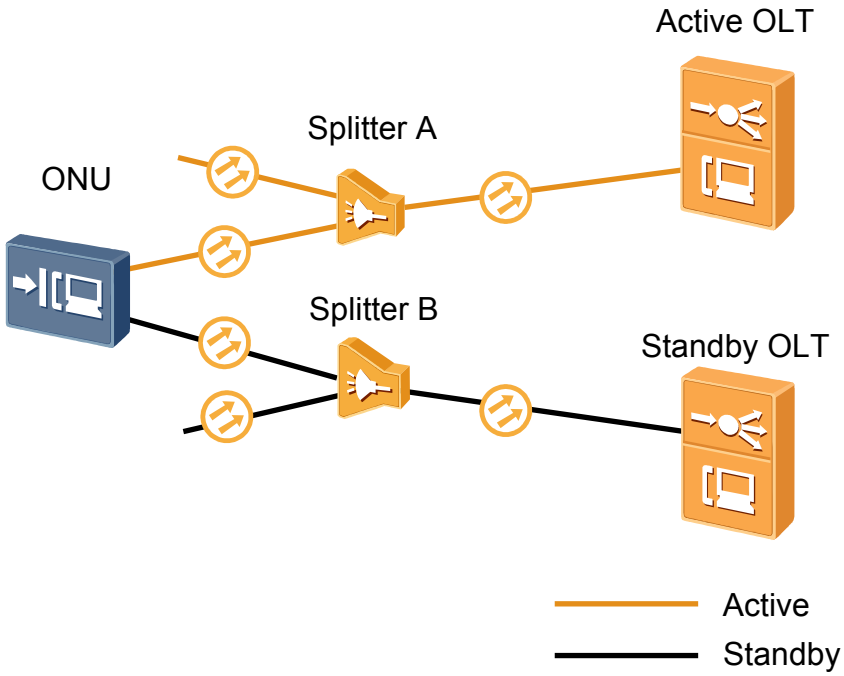
Copyright © Huawei Technologies Co., Ltd.

Figure 12-17 shows the networking diagram for the Type C dual homing protection. Two PON ports on different OLTs, two PON ports on an ONU, two backbone optical fibers, two optical splitters, and two tributary optical fibers are configured to implement this protection. The difference between this protection scheme and the Type C single homing protection scheme is that the ONU needs to be dual homed to two OLTs in this protection scheme.

The models and versions of main control boards on the active and standby OLTs must be the same. The models and versions of GPON boards on the active and standby OLTs also must be the same. Data on the active OLT cannot be automatically synchronized with that on the standby OLT. Therefore, data synchronization between the active and standby OLTs must be manually ensured.

This protection scheme can be configured for only the Ethernet QinQ private line service. It does not support TDM services, including Native TDM and SAToP.

Figure 12-17 Type C dual homing protection



As shown in the preceding figure, Type C dual homing protection is configured for two OLTs (huawei_A and huawei_B).

- huawei_A is the active OLT while huawei_B is the standby OLT.
- The ports on the service boards on both OTLs are 0/3/1.
- The dual homing protection group ID is 1.
- The ONU ID is 1.
- The ONU is authenticated by serial number (SN). The SN of the ONU is 32303131B39FD641 and the management mode is SNMP.
- The ID of the line profile bound to the ONU is 10.

```
Configurations on the active OLT huawei_A:
huawei_A(config)#interface gpon 0/3
huawei_A(config-if-gpon-0/3)#ont add 1 1 sn-auth 32303131B39FD641 snmp ont-
```


Copyright © Huawei Technologies Co., Ltd.

```
lineprofile-id 10
huawei_A(config-if-gpon-0/3)#quit
huawei_A(config)#protect-group 1 protect-target gpon-uni-ont workmode dual-
parenting
huawei_A(protect-group-1)#protect-group member port 0/3/1 ont 1 role work
Configurations on the standby OLT huawei_B:
huawei_B(config)#interface gpon 0/3
huawei_B(config-if-gpon-0/3)#ont add 1 1 sn-auth 32303131B39FD641 snmp ont-
lineprofile-id 10
huawei_B(config-if-gpon-0/3)#quit
huawei_B(config)#protect-group 1 protect-target gpon-uni-ont workmode dual-
parenting
huawei_B(protect-group-1)#protect-group member port 0/3/1 ont 1 role protect
huawei_B(protect-group-1)#protect-group enable
```

----End

12.4.3.7 Verifying Services

This topic describes how to verify the Layer 2 interoperation service by checking the service configurations, service port status, and connectivity between PCs in different branches of an enterprise.

Prerequisites

PCs (with different MAC addresses) connected to different ONUs have been configured. Ensure that the IP addresses of the PCs are in the same network segment or subnet segment.

Procedure

Step 1 Check whether the VLAN configurations are correct.

```
huawei(config)#display vlan 300
{ <cr>|inner-vlan<K>|to<K> }:

  Command:
          display vlan 300
  VLAN ID: 300
  VLAN type: smart
  VLAN attribute: common
  VLAN description:
  VLAN forwarding mode in control board: VLAN-MAC
  VLAN forwarding mode: VLAN-MAC
  VLAN broadcast packet forwarding policy: forward
  VLAN unknown multicast packet forwarding policy: forward
  VLAN unknown unicast packet forwarding policy: forward
  VLAN bind service profile ID: 1
  VLAN bind RAIO profile index: -
  VLAN priority: -
  Standard port number: 0
  -------------------------------------------------------
  INDEX  TYPE  STATE F/ S/ P  VPI  VCI   FLOWTYPE FLOWPARA
  -------------------------------------------------------
     10  gpon  up    0/3 / 1  1    12    vlan     300
     11  gpon  up    0/3 / 1  2    12    vlan     300
  -------------------------------------------------------
  Service virtual port number: 2
  Note: F--Frame, S--Slot, P--Port,
        VPI indicates ONT ID for PON, VCI indicates GEM index for GPON,
        v/e--vlan/encap, pri-tag--priority-tagged
huawei(config)#display vlan service-profile profile-id 1

  Profile   ID: 1
  Profile Name: srvprof-1
```


Copyright © Huawei Technologies Co., Ltd.

```
  ------------------------------------------------------------------------
  Parameter                          Committed          Not Committed
  ------------------------------------------------------------------------
  Forwarding mode                    NotConfig          -
  Anti-macspoofing                   NotConfig          -
  Anti-ipspoofing                    enable             -
  PPPoE MAC mode                     NotConfig          -
  BPDU tunnel                        enable             -
  RIP tunnel                         enable             -
  VTP-CDP tunnel                     enable             -
  DHCP mode                          n/a                -
  DHCP proxy                         enable             -
  DHCP option82                      enable             -
  PITP                               enable             -
  Broadcast packet policy            NotConfig          -
  Multicast packet policy            NotConfig          -
  Unknown unicast packet policy      NotConfig          -
  User-bridging                      enable             -
  IPoE VMAC                          NotConfig          -
  PPPoE VMAC                         NotConfig          -
  PPPoA VMAC                         NotConfig          -
  Mismatch IGMP packet policy        discard            -
  VMAC aging mode                    MAC-learning       -
  OSPF tunnel                        enable             -
  Layer-3 protocol tunnel            enable             -
  MAC-address learning fabric        enable             -
  DHCPv6 mode                        n/a                -
  DHCPv6 option                      enable             -
  PPPoA MAC mode                     NotConfig          -
  Anti-IPv6spoofing                  enable             -
  IPv6 DAD proxy                     disable            -
  Bind route and ND                  disable            -
  NS-reply function                  disable            -
  ARP-reply function                 disable            -
  DHCP relay-interface relay-agent NotConfig            -
  Multicast packet policy fabric     forward            -
  ------------------------------------------------------------------------
  Binding VLAN list            : 300
  ------------------------------------------------------------------------
```

Step 2 Check whether the service port is normal.

```
huawei(config)#display service-port vlan 300
{ <cr>|autosense<K>|sort-by<K> }:

  Command:
          display service-port vlan 300
  Switch-Oriented Flow List
  ------------------------------------------------------------------------------
  INDEX VLAN VLAN     PORT F/ S/ P VPI  VCI   FLOW  FLOW       RX   TX   STATE
        ID   ATTR     TYPE                    TYPE  PARA
  ------------------------------------------------------------------------------
     10  300 common   gpon 0/3 /1  1    12    vlan  300        -    -    up
     11  300 common   gpon 0/3 /1  2    12    vlan  300        -    -    up
  ------------------------------------------------------------------------------
   Total : 2  (Up/Down :    2/0)
huawei(config)#display statistics service-port 10
 Number of upstream bytes             : 1044794
 Number of upstream packets           : 4522
 Number of upstream discard packets   : 200
 Number of downstream bytes           : 1351261
 Number of downstream packets         : 4677
 Number of downstream discard packets : 0
```

Step 3 Check the connectivity between the PCs.

1. Use the PCs to ping each other. If the PCs can ping each other successfully, the PCs are reachable to each other.

Copyright © Huawei Technologies Co., Ltd.

For example, the IP addresses of PC1 and PC2 are 192.168.1.10 and 192.168.1.30 respectively. Ping PC2 on PC1. The expected result is as follows:

```
C:\>ping 192.168.1.30

Pinging 192.168.1.30 with 32 bytes of data:

Reply from 192.168.1.30: bytes=32 time=3ms TTL=128
Reply from 192.168.1.30: bytes=32 time=2ms TTL=128
Reply from 192.168.1.30: bytes=32 time=2ms TTL=128
Reply from 192.168.1.30: bytes=32 time=2ms TTL=128

Ping statistics for 192.168.1.30:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 3ms, Average = 2ms
```

2. You can see one PC in **My Network Places** on the other PC and the two PCs can share data.

----End

Copyright © Huawei Technologies Co., Ltd.

13 FTTO Configuration (Large-sized Enterprise Access)

About This Chapter

Large-sized enterprises generally adopt private line access service. Compared with individual services, this service features various access methods, large number of access users, high security requirement, and cross-region deployment.

NOTE

In this document, the FTTO large-sized enterprise private line access service is written as enterprise access service for short.

13.1 Overview of Enterprise Access Service
This topic describes the basic knowledge about the enterprise access service. Before configuring the enterprise access service, you are advised to learn about the basic knowledge.

13.2 Principle of Planning Data for Enterprise Access Service
This topic plans data for the enterprise access service from multiple dimensions. The data plan guides configuration and optimization of the enterprise service in different scenarios.

13.3 Configuring Enterprise Access Service (GPON)
This topic describes how to configure the enterprise access service in GPON mode in different networking scenarios.

Copyright © Huawei Technologies Co., Ltd.

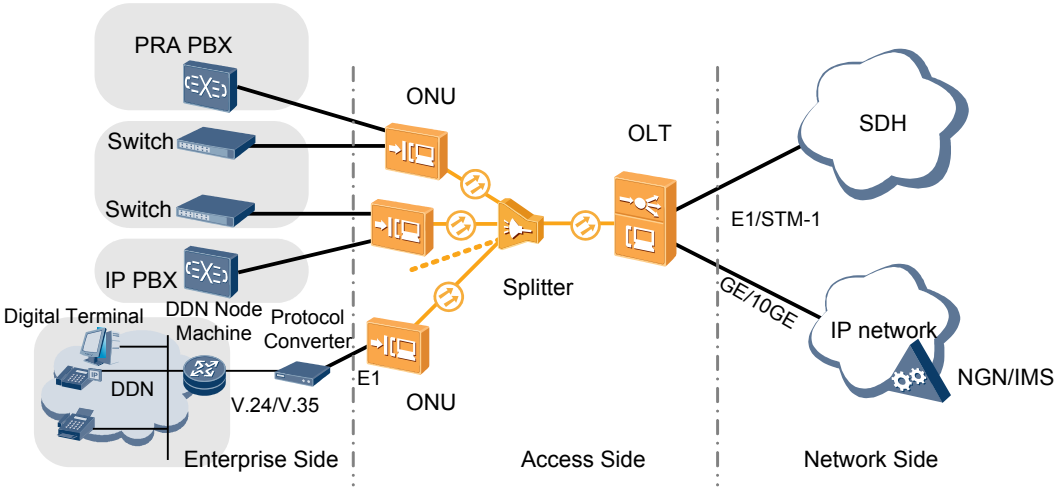
13.1 Overview of Enterprise Access Service

This topic describes the basic knowledge about the enterprise access service. Before configuring the enterprise access service, you are advised to learn about the basic knowledge.

13.1.1 Basic Concepts

The enterprise access solution involves multiple concepts. This topic describes the basic concepts by layers (from the user side to the network side) based on an enterprise access service network diagram.

Network Diagram of Enterprise Access Service



User Side

Concept	Description
IP PBX	IP private branch exchange (PBX) is an IP-based enterprise telephone exchange system. IP PBX uses ICT technology to seamlessly integrate voice communication into the data communication network of an enterprise, simply network architecture, and provide better voice communication between branches of the enterprise.
PRA PBX	PRA PBX, that is, TDM PBX, also called a switch, is a telephone exchange used within an enterprise. With the PRA PBX, staff in the enterprise can use internal telephones to make free calls by dialing short numbers. Outgoing calls are made through a unified trunk. PRA PBX can lower costs and improve work efficiency for the enterprise.

Copyright © Huawei Technologies Co., Ltd.

Concept	Description
DDN	Digital data network (DDN) is a network that uses digital channels to transmit data signals. It provides permanent and semi-permanent connections for users. Compared with traditional analog channels, DDN channels have a higher transmission quality, transmission rate, and bandwidth use rate. DDN is widely used in financial departments, governments, and enterprise groups that require high real-time data switching
DDN node machine	A DDN network consists of backbone node machines and access node machines. A backbone node machine (2M node) implements network service conversion. It provides interfaces and cross-connections for 2 Mbit/s (E1) digital channels, multiplexes and cross-connects Nx64 kbit/s circuit signals, and supports cables reconnection for frame relay services. An access node machine accesses various services for DDN. It provides interfaces for Nx64 kbit/s and 2048 kbit/s digital channels, multiplexes Nx64 kbit/s (N=1–31) signals, and accesses voice and fax users.
Protocol converter	Protocol converter is a device used to convert standard or proprietary protocol of one device to the protocol suitable for the other device or tools to achieve the interoperability. In this document, it implements protocol conversion between V.24/V.35 and E1.

Access Side

Concept	Description
PON	A passive optical network (PON) uses a point-to-multipoint (P2MP) network architecture. A PON network consists of three parts: optical line terminal (OLT), optical distribution network (ODN), and optical network units (ONUs). A PON network uses optical fibers for data transmission, supports more users with less optical fiber resources, and provides a higher access rate. Mainstream PON technologies include broadband passive optical network (BPON), Ethernet passive optical network (EPON), and gigabit passive optical network (GPON).
ODN	The ODN is composed of passive optical components, such as optical fibers and one or more passive optical splitters. The ODN provides highly reliable optical channels between the OLT and ONUs.
OLT	The OLT is an aggregation device located at the central office (CO), which terminates PON protocols. OLTs in this document are MA5600T/MA5603T/MA5608T.

Copyright © Huawei Technologies Co., Ltd.

Concept	Description
ONU	ONUs are located on the user side, providing various types of ports for connecting to user terminals. The ONUs communicate with the OLT through a passive ODN.

Network Side

Concept	Description
SDH	Synchronous digital hierarchy (SDH) is a transmission scheme that follows ITU-T G.707, G.708, and G.709. It defines the transmission features of digital signals such as frame structure, multiplexing mode, transmission rate level, and interface code. SDH is an important part of ISDN and B-ISDN. It interleaves the bytes of low-speed signals to multiplex the signals to high-speed counterparts, and the line coding of scrambling is used only for signals. SDH is suitable for the fiber communications system with high speed and a large capacity since it uses synchronous multiplexing and flexible mapping structure.
NGN/IMS	A next generation network (NGN) is a network that uses softswitches as its core and uses open and standardized architectures to provide abundant services such as VoIP, video, and data. The IP multimedia subsystem (IMS) uses SIP signaling as its call control signaling to provide services such as VoIP, data, and multimedia services. **NOTE** NGN/IMS in this document refers to softswitches that support H.248 and SIP.

Copyright © Huawei Technologies Co., Ltd.

13.1.2 Networking Scenarios and Hardware Configurations (GPON)

Networking Scenarios and Hardware Configurations for Enterprise Access Service (GPON)

Scenario	Scenario Description	Typical OLT Configuration (Main Control Board+Service Board +Upstream Board)	Applicable ONU
Layer 2 interoperation between different enterprise branches	ONUs are deployed in branches of an enterprise. The ONUs access and converge Ethernet services of the enterprise through FE/GE ports and transmit the services to the OLT. The OLT implements Layer 2 interoperation between different branches of the enterprise.	SCUN+GPBC/ GPBD+GICK/ X2CS	MA5612, MA5628
Enterprises DDN private line access	a protocol converter is deployed between an ONU and DDN node machine to convert DDN private line services to E1 services. The ONU accesses the E1 services and encapsulates the service packets in TDM over GEM mode and then transmits the packets to the OLT. The OLT decapsulates the service packets to E1 data and transmits the data to the SDH network through upstream E1/STM-1 ports, achieving transparent transmission of DDN services.	SCUN+GPBC/ GPBD+TOPA For E1 upstream transmission, the TOPA daughter board is NH1A. For STM-1 upstream transmission, the TOPA daughter board is O2CE.	MA5612, MA5628
Enterprise IP PBX access	ONUs access IP PBX services through FE/GE ports. The OLT transparently transmits the data to the IP network in QinQ mode.	SCUN+GPBC/ GPBD+GICK/ X2CS	MA5612, MA5628

Copyright © Huawei Technologies Co., Ltd.

Scenario	Scenario Description	Typical OLT Configuration (Main Control Board+Service Board +Upstream Board)	Applicable ONU
Enterprise PRA PBX access	ONUs access PRA PBX services through E1 lines. The OLT transmits the data to the upper NGN/IMS, achieving the VoIP-based PRA voice service.	SCUN+GPBC/ GPBD+GICK/ X2CS	MA5612
Enterprise E1/T1 unified access	ONU accesses enterprise E1 service through standardized hardware ports, and transmits data to the OLT over the GPON line after performing structure-agnostic time division multiplexing over packet (SAToP) encapsulation on the service. After receiving the signals, the OLT restores E1 signals and transmits the signals to the SDH network.	SCUN+GPBC/ GPBD+EDTB	MA5612, MA5628
Enterprise E1/T1 unified access (OLT Cascading)	ONU accesses the E1/T1 service in SAToP mode, and transmits the service to the OLT at the local site (OLT_B) over the GPON line. OLT_B transparently transmits the service to another OLT with SDH resources (OLT_A) through GE/10GE ports.	OLT_A: SCUN +GPBC/GPBD +EDTB+GICK/ X2CS OLT_B: SCUN +GPBC/GPBD +GICK/X2CS	MA5612, MA5628

13.1.3 GPON ONU Capability Set

This topic describes the supported hardware capability, features, and network position of ONUs on a GPON private line access network.

In FTTx V100R013C00, the MA5612, MA5628 and MA5673 mainly apply to the large-sized enterprise access service. **Table 13-1** shows the ONU capability set.

Copyright © Huawei Technologies Co., Ltd.

Table 13-1 ONU capability set

ONU Type	User Interface	Supported ONU Version
MA5612	For the bottom plate with POTS ports: ● Supports 2xGE electrical interfaces+6xFE electrical interfaces+48xPOTS interfaces+(optional)1xRF interface when two ASNB boards are configured. ● Supports 2xGE electrical interfaces+22xFE electrical interfaces+16xPOTS interfaces+(optional) 1xRF interface when two EIUC boards are configured. ● Supports 2xGE electrical interfaces+6xFE electrical interfaces+16xE1/T1 interfaces+16xPOTS interfaces+(optional)1xRF interface when two E81A boards are configured. For the bottom plate without POTS ports: ● Supports 2xGE electrical interfaces+6xFE electrical interfaces+32xPOTS interfaces when two ASNB boards are configured. ● Supports 2xGE electrical interfaces+22xFE electrical interfaces when two EIUC boards are configured. ● Supports 2xGE electrical interfaces+6xFE electrical interfaces+16xE1/T1 interfaces when two E81A boards are configured.	● V800R308C00 ● V800R308C01 ● V800R310C00 ● V800R311C00 ● V800R312C00
MA5628	There are two types of MA5628: integrated and box-type. Both integrated MA5628 and box-type MA5628 provide: ● 4xE1/T1 interfaces ● 4xGE electrical interfaces	● V800R308C01 ● V800R309C00 ● V800R310C00 ● V800R311C00 ● V800R312C00
MA5673	As a "bridge + Voice" type of ONU, MA5673 provides the following interfaces: ● 4*GE interfaces for Ethernet access ● 4*POTS interfaces for VoIP access ● 4*E1 interfaces for E1 Native TDM leased line access	V800R313C00

Copyright © Huawei Technologies Co., Ltd.

13.2 Principle of Planning Data for Enterprise Access Service

This topic plans data for the enterprise access service from multiple dimensions. The data plan guides configuration and optimization of the enterprise service in different scenarios.

13.2.1 Principle of Equipment Management Data Plan

Data planning for equipment management covers planning of management VLANs and IP addresses.

Management VLAN Planning

- The OLT and ONUs use the same management VLAN.
- The OLT and ONUs use a single SVLAN as the equipment management VLAN.

IP Address Planning

Scenario	IP Address Planning
Equipment management	A management IP address is allocated to each OLT/ONU. Management IP addresses of ONUs connected to the same OLT are usually in the same network segment. Private IP addresses planned by the carrier are used for the purpose of security.
Layer 2 interoperation between different enterprise branches	Enterprise service flows are forwarded at Layer 2 within the FTTx network. Therefore, no IP addresses need to be planned on the OLT and ONUs for enterprise users.
Enterprises DDN private line access	No IP addresses need to be planned because ONUs access the private line service through E1.
Enterprise IP PBX access	No IP addresses need to be planned because the OLT and ONUs provide Layer 2 transparent channels.
Enterprise PRA PBX access	ONUs convert PRA voice signals to H.248 or SIP voice signals. Therefore, the following IP addresses need to be planned: ● Media IP address ● Signaling IP address ● Default gateway IP address
Enterprise E1/T1 unified access	IP addresses are planned as follows: ● On OLTs, source IP addresses of SAToP connections must be planned for EDTB boards. ● On ONUs, source IP addresses of SAToP connections must be planned for E1 boards.

Copyright © Huawei Technologies Co., Ltd.

Scenario	IP Address Planning
Enterprise E1/T1 unified access (OLT Cascading)	These IP addresses are valid only between OLTs and ONUs and therefore can be planned as private IP addresses.

13.2.2 Principle of VLAN Data Plan

VLAN planning for the enterprise access service covers planning of VLANs and VLAN translation policies in different networking scenarios.

VLAN and VLAN Translation Policy

Scenario	VLAN Planning	VLAN Translation	
		ONU	OLT
Layer 2 interoperation between different enterprise branches	● ONUs and the OLT must use single VLAN tags. ● Service flows of the same enterprise has the same VLAN on the OLT. ● Service flows of the same enterprise can have different VLANs on ONUs but the VLANs must be translated to the same VLAN on the OLT.	● The same CVLAN is planned for different branches of an enterprise. ● Different CVLANs are planned for different enterprises.	The OLT allocates a global SVLAN to each enterprise: CVLAN<->SLVAN. **NOTICE** Packets must be forwarded based on VLAN+MAC at Layer 2 instead of SVLAN+CVLAN.
Enterprises DDN private line access	Use a reserved CVLAN (starts from 4000). **NOTICE** A reserved CVLAN cannot be used for Ethernet services on ONUs.	N/A	N/A

Copyright © Huawei Technologies Co., Ltd.

Scenario	VLAN Planning	VLAN Translation	
		ONU	OLT
Enterprise IP PBX access	Single VLAN tag: ONUs and the OLT use single VLAN tags. Service packets are forwarded based on single VLAN tags after being transmitted from the OLT upstream to the metro network. In this way, a large number of VLANs for the metro network will be occupied if there are many OLTs.	1. Different user VLANs are planned for different services (service packets with different destination addresses or paths) of the IP PBX. 2. User VLANs of packets sent from the IP PBX are translated to a specified CVLAN based on service types.	The OLT transparently transmits packets with CVLANs from ONUs.
	(Recommended) Double VLAN tags: Each OLT uses double VLAN tags, an outer VLAN tag (SVLAN) and inner VLAN tag (CVLAN). SLVANs are the same but CLVANs are different. In this way, the number of VLANs required for the metro network is significantly reduced.	1. Different user VLANs are planned for different services (service packets with different destination addresses or paths) of the IP PBX. 2. User VLANs of packets sent from the IP PBX are translated to a specified CVLAN based on service types.	The OLT adds an SVLAN tag: CVLAN<->SVLAN +CVLAN.

Copyright © Huawei Technologies Co., Ltd.

Scenario	VLAN Planning	VLAN Translation	
		ONU	OLT
Enterprise PRA PBX access	(Recommended) Single VLAN tag	ONUs access the PRA PBX through E1, provide the VoIP PRA service, and use the same CVLAN.	The OLT transparently transmits packets.
	Double VLAN tags	ONUs access the PRA PBX through E1, provide the VoIP PRA service, and use the same CVLAN.	The OLT adds an SVLAN tag: CVLAN<->SVLAN +CVLAN.
Enterprise E1/T1 unified access	Plan a global VLAN on the OLT and ONUs, which cannot conflict with other service VLANs.	N/A	N/A
Enterprise E1/T1 unified access (OLT Cascading)			

13.2.3 Principle of QoS Data Plan

QoS planning for the enterprise access service is end-to-end. QoS policies include traffic classification, marking and scheduling, traffic monitoring, and DBA policies. QoS policies for different scenarios are different. This topic provides QoS policies in the following scenarios.

Layer 2 interoperation Between Different Enterprise Branches

Parameter			Value
Traffic classification, marking, and scheduling policies		802.1p priority	4
		Queue scheduling mode	PQ
		OLT queue ID (eight queues)	4
Traffic monitoring and DBA policies	OLT	T-CONT (only for GPON)	An independent T-CONT is used.

Copyright © Huawei Technologies Co., Ltd.

Parameter			Value
		DBA Type	Type 3 ("Assured bandwidth+maximum bandwidth" DBA profile. This type of DBA not only ensures a fixed bandwidth for users but also enables users to preempt a certain amount of bandwidth, but the total bandwidth cannot exceed the maximum bandwidth.)
		DBA bandwidth	Plan the bandwidth according to users' requirements.
		Downstream traffic profile	Configure the profile according to users' bandwidth requirements.
	ONU	Upstream port rate limit	Rates of upstream ports are not limited.
		Downstream port rate limit	Rates of downstream ports are not limited.

Enterprise DDN Private Line Access

In this scenario, ONUs access services from the DDN through E1 lines. Therefore, the QoS policies are mainly planned for traffic on PON lines.

Parameter	Value	Remarks
T-CONT	It is recommended that the number of T-CONTs do not exceed 3. The T-CONT ID ranges from 1 to 3.	It is recommended that all E1 lines of the same ONU use the same T-CONT.
DBA type	Fixed bandwidth and minimum delay	The DBA must be configured properly to achieve low delay, low jitter, and zero packet loss so that the quality of the DDN private line service can be ensured.
DBA bandwidth	Nx7232 kbit/s is recommended. (N is the number of E1 lines.)	It is recommended that the T-CONT ID be 1, 2, or 3 and all E1 lines of the same ONU use the same T-CONT. This setting can leverage bandwidth resources. Each E1 line requires only 5440 kbit/s.

Copyright © Huawei Technologies Co., Ltd.

Enterprise PRA PBX Access

Parameter			Value
Traffic classification, marking, and scheduling policies		802.1p priority	5
		Queue scheduling mode	PQ
		OLT queue ID (eight queues)	5
Traffic monitoring and DBA policies	OLT	T-CONT (only for GPON)	All services share one T-CONT.
		DBA type	Type 3 ("Assured bandwidth+maximum bandwidth" DBA profile. This type of DBA not only ensures a fixed bandwidth for users but also enables users to preempt a certain amount of bandwidth, but the total bandwidth cannot exceed the maximum bandwidth.)
		DBA bandwidth	DBA bandwidth is configured based on the bandwidth package selected by the user. The assured bandwidth is the maximum bandwidth required for transmitting management packets and VoIP service packets. The maximum bandwidth is equal to or higher than the maximum bandwidth applied by the user.
		Downstream traffic profile	Downstream traffic rate is not limited.
	ONU	Upstream port rate limit	Set this parameter based on requirements.
		Downstream port rate limit	Set this parameter based on requirements.

Enterprise IP PBX Access

The QoS policies for this scenario are the same as those for the **Layer 2 interoperation Between Different Enterprise Branches** scenario.

Enterprise E1/T1 unified access

In this scenario, ONUs access services through E1/T1 lines. Therefore, the QoS policies are mainly planned for traffic on PON lines.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Value	Remarks
T-CONT	It is recommended that the number of T-CONTs do not exceed 3. The T-CONT ID ranges from 1 to 3.	It is recommended that all E1 lines of the same ONU use the same T-CONT.
DBA type	Fixed bandwidth and minimum delay	The DBA must be configured properly to achieve low delay, low jitter, and zero packet loss so that the quality of the T1 base station access service can be ensured.
DBA bandwidth	● E1 access: Nx8 Mbit/s is recommended. (N is the number of E1 lines.) ● T1 access: Nx6 Mbit/s is recommended. (N is the number of E1 lines.)	-

Enterprise E1/T1 unified access (OLT Cascading)

The QoS policies for this scenario are the same as those for the **Enterprise E1/T1 unified access** scenario.

13.2.4 Principle of Protocol Transparent Transmission Data Plan

The enterprise access service involves transparent transmission of protocol packets. Different equipment configurations are required for transparently transmitting different protocol packets.

Configurations for Protocol Transparent Transmission

Protocol Type	Protocol Description	Configuration (remarks 1)

BPDU	STP, MSTP, RSTP, IS-IS	The function of transparently transmitting BPDU packets must be enabled.
		Configuration example:
		`huawei(config)#vlan service-profile profile-id 1`
		`huawei(config-vlan-srvprof-1)#bpdu tunnel enable`

ETH OAM	IEEE 802.1ag	No configuration is required because packets are transparently transmitted by hardware.
Broadcast	ARP	No configuration is required because packets are transparently transmitted by hardware.
Layer 2/Layer 3 protocol	NTP, BGP, LDP, RSVP, IGMP, PIM	No configuration is required because packets are transparently transmitted by hardware.

Copyright © Huawei Technologies Co., Ltd.

Protocol Type	Protocol Description	Configuration (remarks 1)

	OSPF	The function of transparently transmitting OSPF packets must be enabled.
		Configuration example:
		`huawei(config)#vlan service-profile profile-id 1`
		`huawei(config-vlan-srvprof-1)#ospf tunnel enable`

	RIP	The function of transparently transmitting RIP packets must be enabled.
		Configuration example:
		`huawei(config)#vlan service-profile profile-id 1`
		`huawei(config-vlan-srvprof-1)#rip tunnel enable`

VTP/CDP	VTP/CDP protocol is a proprietary protocol of other vendors. It is used to discover neighbors and establish neighbor relationship.	The function of transparently transmitting VTP/CDP packets must be enabled.
		Configuration example:
		`huawei(config)#vlan service-profile profile-id 1`
		`huawei(config-vlan-srvprof-1)#vtp-cdp tunnel enable`

Unknown multicast	Planned by carriers for special purposes	The function of transparently transmitting unknown multicast packets must be enabled. Configuration example: `huawei(config)#multicast-unknown policy service-port 1 transparent`

Remarks 1: The configurations take effect only after the configured VLAN service profile is bound to a VLAN. Command: **vlan bind service-profile** *vlan-id profile-id*

13.2.5 Principle of Security Data Plan

Security planning covers planning of system security, user security, and service security data. An appropriate security plan ensures normal running of services.

NOTE

- The device provides complete security measures, but not all security measures need to be deployed. Only the security measures that meet the following requirements need to be deployed:
  - The security measures can be used on the live network.
  - The security measures are easy to deploy.
  - The security measures are effective.
- Different ONUs support different security features. Select the security feature recommended in this topic according to actual ONU capabilities.

Copyright © Huawei Technologies Co., Ltd.

System Security

Security Vulnerability	Solution	Description and Usage Suggestion
DoS attack	Enable the anti-DoS-attack function for OLT and MDU.	After the anti-DoS-attack function is enabled, control packets are monitored and those exceeding the number threshold are discarded. Use this solution for new site deployment.
IP attack	Enable the anti-IP-attack function for OLT and MDU.	After the anti-IP-attack function is enabled, a device discards the IP packets received from the user side whose destination IP address is the IP address of the device, and therefore the system is protected. Use this solution for new site deployment.

User Security

Security Vulnerability	Solution	Description and Usage Suggestion
MAC spoofing	Enable the anti-MAC-duplicate function for OLT and MDU.	After anti-MAC-duplicate is enabled, the system records the first MAC address learnt from the port and binds the MAC address to the port and VLAN. If receiving packets sent from the host that has the same MAC address with the port, the system discards the packets directly. In this case, it can prevent users from forging MAC addresses to perform malicious attacks. Use this solution for new site deployment.
MAC attack	Enable the anti-MAC spoofing function for OLT and MDU.	After anti-MAC spoofing is enabled, the system can prevent users from forging IP addresses to perform malicious attacks. Use this solution for new site deployment.

Copyright © Huawei Technologies Co., Ltd.

Security Vulnerability	Solution	Description and Usage Suggestion
IP spoofing	Enable the anti-IP spoofing function for MDU.	After anti-IP spoofing is enabled, the system can prevent users from forging IP addresses to perform malicious attacks. Use this solution for new site deployment.

13.2.6 Principle of Reliability Data Plan

Reliability planning covers planning of equipment reliability and upstream/downstream networking protection. Reliability planning helps to achieve high reliability of private line services.

Equipment Reliability

Protection Scheme	Description	Suggestion
Main control board 1 +1 protection	The system uses two main control boards of the same model and version. The two main control boards work in the active/standby mode by default. When the active main control board fails, the system switches to the standby main control board to prevent service interruption.	Mandatory
Power board 1+1 protection	A subrack is configured with two power boards of the same model and version, which back up each other. When one of the power board fails, the other power board can still provide power supply to the device and so the system can still work properly.	Mandatory
Upstream board 1+1 protection	The system uses two upstream interface boards of the same model and version. Each GIU board provides one upstream port and two upstream ports are bound together using Link Aggregation Control Protocol (LACP). When the active upstream port fails, traffic will be transmitted upstream through the standby upstream port.	This protection scheme is recommended when the GIU board is used to transmit traffic upstream.

Copyright © Huawei Technologies Co., Ltd.

Upstream Networking Protection

Protection Scheme	Description	Suggestion
Link aggregation group	Multiple Ethernet ports are bound together as an aggregation group to increase the bandwidth and balance the inbound and outbound load of each member port. In addition, the ports in an aggregation group back up each other, which enhances the reliability of links.	This protection scheme is mandatory when the GIU board is used to transmit traffic upstream.
Protection group (Ethernet/STM-1)	A protection group of upstream ports contains a working port and a protection port. In normal state, the working port carries services and the protection port does not. When the link at the working port is faulty, the system automatically switches services from the working port to the protection port to ensure normal service transmission and protect the uplink.	When the main control board is used to transmit traffic upstream, this protection scheme is mandatory. This protection scheme is recommended when traffic is transmitted upstream through STM-1 ports.

NOTE

Link aggregation group and Ethernet protection group usually are not configured at the same time. You are advised to configure only one of the two protection schemes.

Downstream Networking Protection

Protection Scheme	Description	Suggestion
xPON Type B	Two PON ports on the same OLT back up each other. When one of the PON ports fails, the system automatically switches to the other PON port. This protection scheme provides port-level protection with low costs. It protects services against fiber failure at the working port.	It rovides port-level protection and has a low cost. The inter-board protection mode is recommended.
GPON Type C single homing	Two PON ports on the same OLT, two PON ports on an ONU, two backbone optical fibers, two optical splitters, and two tributary optical fibers are configured to provide link-level protection.	It rovides link-level protection.

Copyright © Huawei Technologies Co., Ltd.

Protection Scheme	Description	Suggestion
GPON Type C dual homing	Two PON ports on different OLTs, two PON ports on an ONU, two backbone optical fibers, two optical splitters, and two tributary optical fibers are configured to implement this protection. The difference between this protection scheme and the GPON Type C single homing protection scheme is that the ONU needs to be dual homed to two OLTs in this protection scheme. This full-backup protection scheme provides the highest-level protection for links and has the highest costs.	It provides full backup protection, which is the highest level of protection, at the same time, it has the highest cost. This protection scheme can be configured for only the Ethernet QinQ private line service. It does not support TDM services, including Native TDM and SAToP.

NOTE

The Type B protection scheme, Type C single homing scheme, and Type C dual homing protection scheme are mutually exclusive. Therefore, only one of these protection schemes can be configured for an ONU.

13.3 Configuring Enterprise Access Service (GPON)

This topic describes how to configure the enterprise access service in GPON mode in different networking scenarios.

Context

There are two xPON configuration modes: distributed mode (also called discrete mode) and profile mode. The difference between the two modes lies in command lines.

- Distributed mode: In this mode, ONTs need to be configured one by one but not in batches.
- Profile mode: In this mode, an ONT line profile and service profile are configured first. Then, ONTs can be added in batches by binding profiles. This mode greatly improves service provisioning efficiency.

Generally, the xPON configuration mode is determined in a new deployment and will not be changed. This chapter describes how to configure the enterprise access service in PON profile mode (which is the default mode). You can run the commands in the following table to query the xPON configuration mode.

Mode	Query Method
PON profile mode	huawei(config)#**diagnose** huawei(diagnose)%%**display xpon mode** --- Current config mode: Profile-mode ---

Copyright © Huawei Technologies Co., Ltd.

NOTE

For commands for the distributed configuration mode, see **PON distributed-mode commands** in the *Command Reference*.

13.3.1 Layer 2 Interoperation Service Between Enterprise Branches

Different branches of an enterprise can achieve Layer 2 interoperation through ONUs. Then, different branches can transmit service traffic to each other just like in the same LAN, which can improve coordination work efficiency.

13.3.1.1 Service Requirement and Application Scenario

Service Requirement

An enterprise that has multiple branches requires intercommunication between different branches or between its headquarter and branches. Virtual private network (VPN) can achieve secure interconnection but requires additional devices and complex management. It requires high costs even if a leased VPN is used. In addition, the bandwidth provided by a VPN is limited due to restricted VPN access modes and the bandwidth control is inflexible.

To address the preceding problems, the Layer 2 interoperation technology using fiber access is put forward and becomes the main trend.

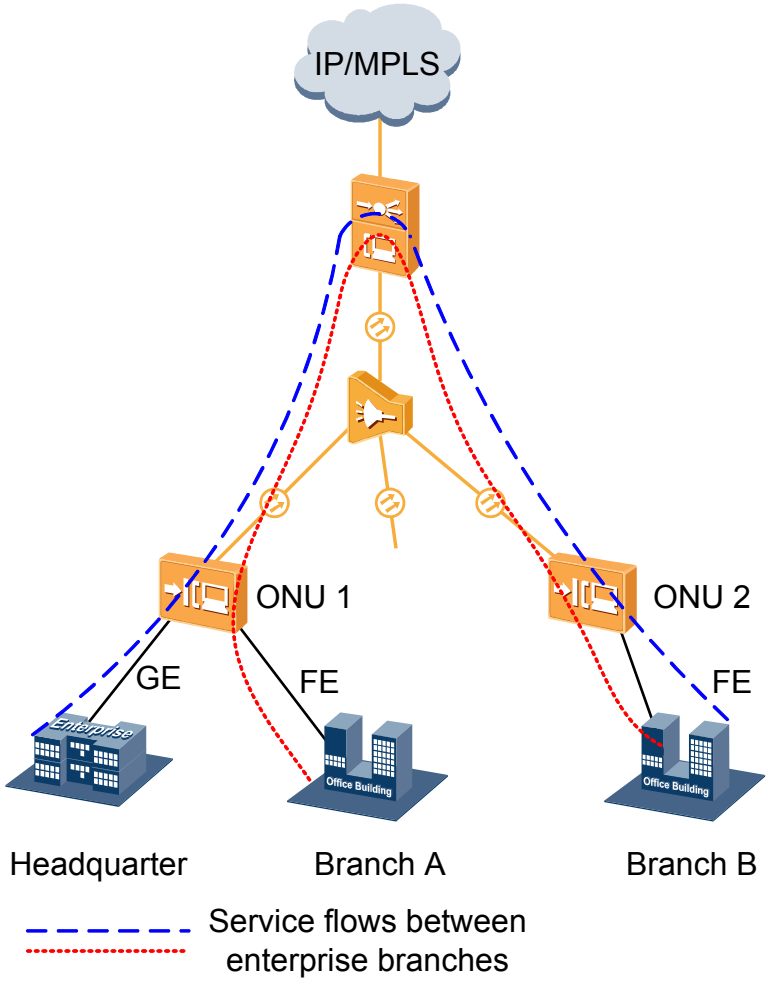
Application Scenario

As shown in **Figure 13-1**, ONUs are deployed in branches of an enterprise. The ONUs access and converge Ethernet services of the enterprise through FE/GE ports and transmit the services to the OLT. The OLT implements Layer 2 interoperation between different branches of the enterprise.

ONUs supporting this scenario: MA5612, MA5628, MA5616

Copyright © Huawei Technologies Co., Ltd.

Figure 13-1 Network diagram for Layer 2 interoperation between enterprise branches



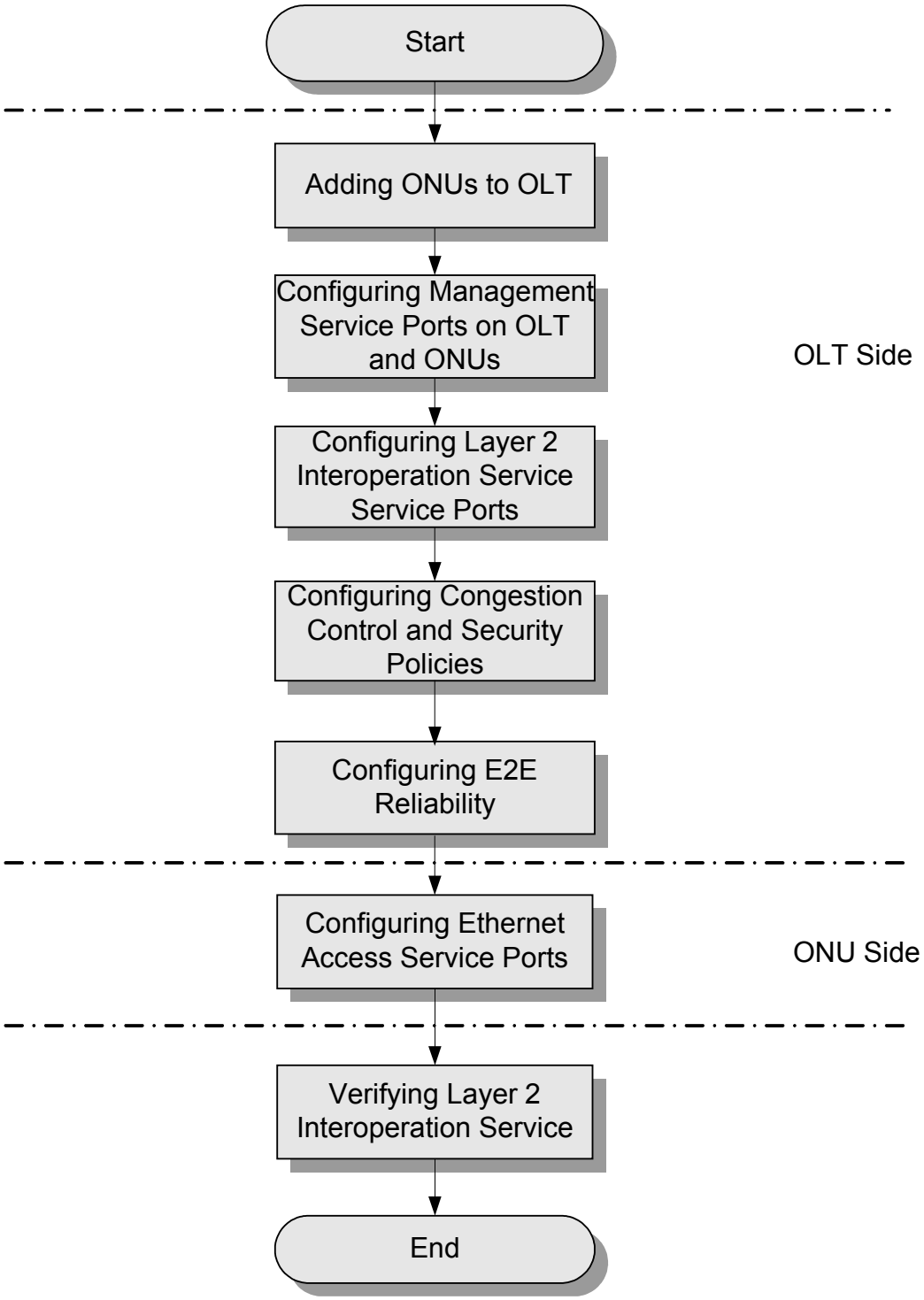
Note: Because the bandwidth of upstream and downstream PON ports is fixed, the number of enterprises connected to an OLT is limited when the enterprises require symmetric bandwidth. When an enterprise requires 100 Mbit/s symmetric bandwidth:

1. The number of enterprises or branches connected to a PON port should not exceed eight.
2. The number of enterprises or branches connected to a PON board should not exceed 64.
3. The number of enterprises connected to an OLT cannot exceed 200 (20G/100M) if the upstream bandwidth is 2x10GE. (The number of enterprises connected to an OLT is mainly restricted by the upstream bandwidth.)

13.3.1.2 Configuration Process

The following figure shows the configuration process for Layer 2 interoperation between branches of an enterprise.

Copyright © Huawei Technologies Co., Ltd.



NOTE

An OLT can connect to multiple ONUs (for enterprise branches). Configurations for different ONUs are similar. Therefore, this document uses two ONUs (ONU1 and ONU2) as example to describe how to configure Layer 2 interoperation.

13.3.1.3 Adding ONUs to OLT

This topic describes how to add ONUs to the OLT. ONUs can be configured only after they are added to the OLT successfully.

Copyright © Huawei Technologies Co., Ltd.

Context

- When adding ONUs, you need to bind related profiles to the ONUs, including the DBA profile, line profile, and alarm profile. For the functions of each profile and how to configure profiles, see **Table 13-2**.

Table 13-2 ONU profile

Profile Type	Function	Command
DBA profile	Describes GPON traffic parameters. A T-CONT is bound to a DBA profile for dynamic bandwidth allocation, improving upstream bandwidth utilization.	Query: **display dba-profile** Add: **dba-profile add**
Line profile	Describes the binding relationship between T-CONTs and DBA profiles, QoS mode of service flows, and mapping between GEM ports and services on ONUs.	Query: **display ont-lineprofile** Add: **ont-lineprofile add**
Alarm profile	Provides a series of alarm threshold parameters that are used for performance measurement and monitoring of activated ONU lines.	Query: **display gpon alarm-profile** Add: **gpon alarm-profile add**

- An ONU can be added in two modes. Select either mode as required.

Mode	Application Scenario	Command
Offline addition	The password or serial number of an ONU has been obtained.	Run the **ont add** command to add the ONU.
Online confirmation	The password and serial number of an ONU are unknown.	Run the **port ont-auto-find** command in the GPON mode to enable the automatic discovery function for the GPON port and run the **ont confirm** command to add the ONU.

Copyright © Huawei Technologies Co., Ltd.

Data Planning

Table 13-3 Key data plan

Configuration Item	Data
DBA profile	Profile ID: 20 Profile type: Type 3 Assured bandwidth: 100 Mbit/s Maximum bandwidth: 120 Mbit/s
Line profile	Profile ID: 10 T-CONT ID: 4 GEM port ID for management service: 11 GEM port ID for Layer 2 interoperation service: 12
Networking data	For example, add two ONUs (ONU 1 and ONU 2) for carrying services of different branches. ● ONU 1 is connected to PON port 0/3/1. ● ONU 2 is connected to PON port 0/4/1.

Procedure

Step 1 Configure GPON ONU profiles.

1. Configure a DBA profile.

```
huawei(config)#dba-profile add profile-id 20 type3 assure 102400 max 122880
```

2. Configure an ONU line profile.

   a. Create GPON ONU line profile 10.

```
huawei(config)#ont-lineprofile gpon profile-id 10
```

   NOTE

   Create a line profile according to the data plan. The ID of the line profile to be created cannot conflict with existing profile IDs in the system. In this example, the ID of the line profile is 10.

   b. In the line profile configuration mode, bind T-CONT 4 to DBA profile 20.

```
huawei(config-gpon-lineprofile-10)#tcont 4 dba-profile-id 20
```

   c. In the line profile configuration mode, bind GEM ports to T-CONTs.

   - Add GEM port 11 for carrying the management service flow.
   - Add GEM port 12 for carrying the Layer 2 interoperation service flow.

   Both GEM port 11 and GEM port 12 are bound to T-CONT 4. During configuration, set QoS policies for each service flow. For details on QoS data planning, see **13.2.3 Principle of QoS Data Plan**.

```
huawei(config-gpon-lineprofile-10)#gem add 11 eth tcont 4 cascade on
huawei(config-gpon-lineprofile-10)#gem add 12 eth tcont 4 cascade on
```

   d. Configure mapping between GEM ports and ONU-side services.

Copyright © Huawei Technologies Co., Ltd.

Set the mapping mode to VLAN mode (the default mode). Map the management service flow (CVLAN 8) to GEM port 11, and map Layer 2 interoperation service flow (CVLAN 300) to GEM port 12.

```
huawei(config-gpon-lineprofile-10)#gem mapping 11 0 vlan 8
huawei(config-gpon-lineprofile-10)#gem mapping 12 1 vlan 300
```

e. After the configuration is complete, run the **commit** command to make the configured parameters take effect.

```
huawei(config-gpon-lineprofile-10)#commit
huawei(config-gpon-lineprofile-10)#quit
```

3. (Optional) Configure an alarm profile.
   - The default GPON alarm profile ID is 1. The value of each alarm threshold is **0** which indicates that alarms are not reported.
   - In this example, the default alarm profile is used and no configuration is required.

Step 2 Add ONUs to the OLT.

1. Add ONU 1 and ONU2 in offline mode.

   Connect ONU 1 and ONU 2 to GPON ports 0/3/1 and 0/4/1 respectively through an optical splitter. The serial numbers of the two ONUs are 32303131B39FD641 and 32303131B39FD642 respectively, and the management mode is SNMP. Both the ONUs are bound to line profile 10.

```
huawei(config)#interface gpon 0/3
huawei(config-if-gpon-0/3)#ont add 1 ontid 1 sn-auth 32303131B39FD641
snmp ont-lineprofile-id 10
huawei(config-if-gpon-0/3)#quit
huawei(config)#interface gpon 0/4
huawei(config-if-gpon-0/4)#ont add 1 ontid 2 sn-auth 32303131B39FD642
snmp ont-lineprofile-id 10
```

2. (Optional) Bind an alarm profile.

   By default, an ONU will be automatically bound to alarm profile 1 (default profile). You need to manually bind an alarm profile to an ONU only when the default alarm profile does not meet requirements.

   In this example, the default alarm profile is used. Therefore, you do not need to manually bind an alarm profile.

Step 3 Confirm the ONU status.

After adding an ONU, run the **display ont info** command to query the current status of the ONU. Ensure that **Control flag** is **active**, **Run State** is **online**, and **Config state** is **normal**.

The following uses ONU 1 as an example to describe how to confirm ONU status.

```
huawei(config-if-gpon-0/3)#display ont info 1 1
  ------------------------------------------------------------------------
  F/S/P                : 0/3/1
  ONT-ID               : 1
  Control flag         : active    //Indicates that the ONU is
activated.
  Run state            : online    //Indicates that the ONU is
online.
  Config state         : normal    //Indicates that the ONU is in normal
state.
...//Other command output is omitted.
huawei(config-if-gpon-0/3)#quit
```

----End

Copyright © Huawei Technologies Co., Ltd.

Follow-up Procedure

When **Config state** is **failed**, **Run state** is **offline**, or **Match state** is **mismatch**:

- If **Control flag** is **deactive**, run the **ont active** command in GPON mode to activate the ONU.
- If **Run state** is **offline**, a physical line may be broken or the optical module may be damaged. Check the line and the optical module.
- If **Config state** is **failed**, the configured ONU capability exceeds the actual ONU capability. In this case, run the **display ont failed-configuration** command in the diagnose mode to check the failed configuration item and the failure cause. Then, rectify the fault accordingly.
- If the ONU does not match, that is, **Match state** is **mismatch**, the port types and number of ports undermatch the actual port types and number of ports supported by the ONU. In this case, run the **display ont capability** command to query the actual capability of the ONU, and then select one of the following modes to modify the ONU configuration:
  - Create a proper ONU profile according to the actual capability of the ONU, and then run the **ont modify** command to modify the configuration data of the ONU.
  - Modify the ONU profile according to the actual capability of the ONU and save the modification. Then, the ONU automatically recovers the configuration successfully.

13.3.1.4 Configuring Management Service Ports on OLT and ONUs

This topic describes how to configure management service ports (also called service flows) on the OLT and ONUs. After the connections between the in-band management service ports on the OLT and ONUs are reachable, you can log in to the ONUs on the OLT and configure the ONUs.

Data Plan

Configuration Item	Data
Management VLAN and management IP address for OLT	Management VLAN ID: 8 Management VLAN type: smart In-band management IP address: 192.168.50.1/24
Management VLAN and management IP address for ONU	Management VLAN ID: 8 Management VLAN type: smart In-band management IP address for ONU 1: 192.168.50.2/24 In-band management IP address for ONU 2: 192.168.50.3/24

NOTE

To log in to and configure an ONU remotely on the OLT, the management VLAN of the OLT must be the same as that of the ONU, and the management IP address of the OLT and that of the ONU must be in the same network segment.

Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Configure the in-band management VLAN and IP address for the OLT.

Set the in-band management VLAN to 8, VLAN priority to 6, and IP address to 192.168.50.1/24.

```
huawei(config)#vlan 8 smart
huawei(config)#port vlan 8 0/19 0
huawei(config)#vlan priority 8 6
huawei(config)#interface vlanif 8
huawei(config-if-vlanif8)#ip address 192.168.50.1 24
huawei(config-if-vlanif8)#quit
```

Step 2 Configure the in-band management VLAN and IP addresses for the ONUs.

Set the static IP address to 192.168.50.2/24 for ONU1, 192.168.50.3/24 for ONU2, the gateway IP address to 192.168.50.1, and management VLAN to 8 (which is the same as that of the OLT).

```
huawei(config)#interface gpon 0/3
huawei(config-if-gpon-0/3)#ont ipconfig 1 1 static ip-address 192.168.50.2 mask
255.255.255.0 gateway
192.168.50.1 vlan 8
huawei(config-if-gpon-0/3)#quit
huawei(config)#interface gpon 0/4
huawei(config-if-gpon-0/4)#ont ipconfig 1 2 static ip-address 192.168.50.3 mask
255.255.255.0 gateway
192.168.50.1 vlan 8
huawei(config-if-gpon-0/4)#quit
```

Step 3 Configure the in-band management service port.

Set the management VLAN to 8, GEM port ID to 11, and user VLAN to 8. The OLT does not rate limit the in-band management service port. Therefore, directly use the default traffic profile 6.

```
huawei(config)#service-port vlan 8 gpon 0/3/1 ont 1 gemport 11 multi-service
user-vlan 8 rx-cttr 6 tx-cttr 6
huawei(config)#service-port vlan 8 gpon 0/4/1 ont 2 gemport 11 multi-service
user-vlan 8 rx-cttr 6 tx-cttr 6
```

Step 4 Confirm that the connections between the management service ports on the OLT and ONUs are reachable.

- Run the **ping *ONU ip*** command on the OLT to verify the connectivity between the OLT and ONUs. If the OLT receives ICMP ECHO-REPLY packets from the ONUs, the connection is reachable.
- When the connection is reachable, you can remote log in to the ONU from the OLT and configure the ONUs.

----End

13.3.1.5 Configuring Layer 2 Interoperation Service Ports on OLT

This topic describes how to configure service ports on the OLT for Layer 2 interoperation so that data packets sent from different ONUs can be forwarded based on the same VLAN at Layer 2.

Prerequisites

1. The main control board on the device is an SCUN board.

Copyright © Huawei Technologies Co., Ltd.

2. The ARP proxy function is disabled using the **arp proxy disable** command. (The Layer 2 interoperation function and ARP proxy function are mutually exclusive.)

Data Plan

Configuration Item	Data
Layer 2 interoperation SVLAN	OLT VLAN ID (the OLT transparently transmits VLANs of ONU): 300 VLAN forwarding mode: vlan-mac (default) ONU VLAN ID: 300 Service flow ID: 301
Traffic profile	Profile ID: 10 Assured bandwidth: 100 Mbit/s Priority source: user-cos Default priority: 4

NOTE

For detailed data planning, see **13.2.2 Principle of VLAN Data Plan**.

Procedure

Step 1 Configure an SVLAN and add an upstream port to it.

Set the SVLAN ID of the Layer 2 interoperation service to 300, VLAN type to smart VLAN, and add upstream port 0/19/0 to the VLAN.

```
huawei(config)#vlan 300 smart
huawei(config)#port vlan 300 0/19 0
```

Step 2 Configure a traffic profile.

Add a new traffic profile 10 and set the assured rate to 100 Mbit/s. Packets transmitted upstream use the priority (4 by default) copied from the user side. Packets transmitted downstream use the priority carried by themselves.

```
huawei(config)#traffic table ip index 10 cir 102400 priority user-cos 4 priority-policy tag-in-package
```

Step 3 Configure a service port to receive and transparently transmit the Layer 2 interoperation service that is sent from ONU 1 and ONU 2.

Set the service attributes based on the data plan:

- For the OLT, set the SVLAN ID to 300, CVLAN ID to 300 which is the same as the upstream VLAN ID of the ONU, and GEM port ID to 12 for the Layer 2 interoperation service.
- For ONUs, set the upstream VLAN ID to 300.

```
huawei(config)#service-port 301 vlan 300 gpon 0/3/1 ont 1 gemport 12 multi-service
user-vlan 300 rx-cttr 10 tx-cttr 10
huawei(config)#service-port 302 vlan 300 gpon 0/4/1 ont 2 gemport 12 multi-
```


Copyright © Huawei Technologies Co., Ltd.

```
service
user-vlan 300 rx-cttr 10 tx-cttr 10
```

Step 4 Configure attributes for protocol transparent transmission.

Create a VLAN service profile, enable the VLAN Layer 2 interoperation function, and configure attributes for protocol transparent transmission. Then, bind the profile to VLAN 300. For details on data planning for protocol transparent transmission, see **13.2.4 Principle of Protocol Transparent Transmission Data Plan**.

```
huawei(config)#vlan service-profile profile-id 1
huawei(config-vlan-srvprof-1)#user-bridging enable   //Mandatory
huawei(config-vlan-srvprof-1)#bpdu tunnel enable
huawei(config-vlan-srvprof-1)#ospf tunnel enable
huawei(config-vlan-srvprof-1)#rip tunnel enable
huawei(config-vlan-srvprof-1)#vtp-cdp tunnel enable
huawei(config-vlan-srvprof-1)#commit
huawei(config-vlan-srvprof-1)#quit
huawei(config)#multicast-unknown policy service-port 301 transparent
huawei(config)#multicast-unknown policy service-port 302 transparent
huawei(config)#vlan bind service-profile 300 profile-id 1
```

----End

13.3.1.6 Configuring Ethernet Access Service Ports on ONUs

This topic describes how to configure service ports on ONUs and configure upstream VLANs to make the ONU-to-user connection reachable and create ONU-to-OLT upstream data channels.

Data Planning

Configuration Item	Data
Port	Upstream port: 0/0/1 Service port: 0/3/1
SVLAN	VLAN ID: 300 VLAN type: smart VLAN attribute: common
Traffic profile	Profile ID: 8 Assured rate: no rate limit Priority source: user-cos Default riority: 4

NOTE

Data plans for ONU1 and ONU 2 are the same. This topic uses one ONU as an example to describe how to configure the ONU.

Procedure

Step 1 Remotely log in to an ONU to configure the ONU.

Copyright © Huawei Technologies Co., Ltd.

You can remote log in to the ONU from the OLT to perform the configuration. User name: **root** (default); password: **mduadmin** (default)

Step 2 Create an SVLAN and add an upstream port to the VLAN.

```
huawei(config)#vlan 300 smart
huawei(config)#port vlan 300 0/0 1
```

Step 3 Configure a traffic profile.

Configure traffic profile 8. The upstream and downstream rates are not limited. Packets transmitted upstream use the priority (4 by default) copied from the user side. Packets transmitted downstream use the priority carried by themselves.

```
huawei(config)#traffic table ip index 8 cir off priority user-cos 4 priority-policy tag-in-package
```

Step 4 Add a service port.

Add service port 301 and bind it to port 0/3/1. Set the user VLAN to untagged and bind it to traffic profile 8.

```
huawei(config)#service-port 301 vlan 300 eth 0/3/1 multi-service user-vlan untagged rx-cttr 8 tx-cttr 8
```

NOTE

Packets sent from the user side (enterprise branches) may be transmitted upstream with a VLAN tag. In this case, change **untagged** to the VLAN tag when configuring a service port.

----End

13.3.1.7 Configuring Congestion Control and Security Policies

This topic describes how to configure global priority-based scheduling policies for queues to ensure service reliability and configure global security policies to ensure service security.

Context

Congestion control uses queue scheduling technology to map packets sent from the same port into multiple queues and process packets in each queue based on priority. Congestion control is recommended.

Security policies cover system security, user security, and service security, which ensure normal running of services.

NOTE

Enable security features based on service types. For details, see **13.2.5 Principle of Security Data Plan**.

Procedure

- Configure queue scheduling.

  Based on **13.2.3 Principle of QoS Data Plan**, all packets use strict priorities for queue scheduling and are mapped to queues based on priorities.

  ```
  huawei(config)#queue-scheduler strict-priority
  huawei(config)#cos-queue-map cos0 0 cos1 1 cos2 2 cos3 3 cos4 4 cos5 5 cos6 6 cos7 7  //System default
  ```

- Configure system security.
  - Enable deny of service (DoS) anti-attack on both the OLT and optical network units (ONUs).

Copyright © Huawei Technologies Co., Ltd.

1. Run the **security anti-dos enable** command to globally enable DoS anti-attack.
2. Run the **security anti-dos control-packet policy** command to configure a protocol packet processing policy that will be used when a DoS attack occurs.
3. Run the **security anti-dos control-packet rate** command to configure the threshold for the rate of sending protocol packets to the CPU.

- Enable IP address anti-attack on both the OLT and ONUs.

  Run the **security anti-ipattack enable** command to enable IP address anti-attack.

- Configure user security.
  - Enable MAC address anti-flapping on both the OLT and ONUs.

    Run the **security anti-macduplicate enable** command to enable MAC address anti-flapping.
  - Enable MAC address anti-spoofing on both the OLT and ONUs.

    1. In global config mode, run the **security anti-macspoofing enable** command to globally enable MAC address anti-spoofing.
    2. Enable MAC address anti-spoofing at VLAN level in global config mode or service profile mode:
       a. In global config mode, run the **security anti-macspoofing vlan** command to enable MAC address anti-spoofing.
       b. Perform the following operations to enable MAC address anti-spoofing in service profile mode:
          a. In global config mode, run the **vlan service-profile** command to create a VLAN service profile.
          b. Run the **security anti-macspoofing enable** command to enable MAC address anti-spoofing at VLAN level.
          c. Run the **commit** command to make the profile configuration take effect.
          d. Run the **quit** command to quit the VLAN service profile mode.
          e. Run the **vlan bind service-profile** command to bind the created VLAN service profile to a VLAN.
    3. (Optional) Run the **security anti-macspoofing max-mac-count** command to set the maximum number of MAC addresses that can be bound to a service flow.
    4. (Optional) Run the **security anti-macspoofing exclude** command to configure the types of packets for which MAC address anti-spoofing does not take effect, such as Internet Group Management Protocol (IGMP) packets.
  - Enable IP address anti-spoofing on ONUs.

    IP address anti-spoofing can be enabled or disabled at three levels: global, VLAN, and service port levels. This function takes effect only after it is enabled at the three levels. Among the three levels, IP address anti-spoofing is disabled only at the global level by default.

    1. In global config mode, run the **security anti-ipspoofing enable** command to enable IP address anti-spoofing at the global level.
    2. In VLAN service profile mode, run the **security anti-ipspoofing enable** command to enable IP address anti-spoofing at the VLAN level.

Copyright © Huawei Technologies Co., Ltd.

3. Run the **security anti-ipspoofing service-port** *serviceport-id* **enable** command to enable IP address anti-spoofing at the service port level.

----End

13.3.1.8 Configuring E2E Reliability

This topic describes how to configure end-to-end (E2E) protection schemes for the enterprise private line service which has a high requirement on service reliability.

Context

Reliability covers equipment reliability, upstream networking protection, and downstream networking protection. For details on reliability data planning, see **13.2.6 Principle of Reliability Data Plan**.

- Upstream networking protection includes link aggregation group and protection group. Usually, link aggregation group is configured when the GIU board is used to transmit traffic upstream; protection group is configured when the main control board is used to transmit traffic upstream. The two protection schemes are not configured at the same time.
- Downstream networking protection includes Type B, Type C single homing, and Type C dual homing, which are used to protect service ports. Ports on the same ONU can be configured only with the same protection scheme.

NOTE

This topic describes how to configure five mainstream protection schemes. Select required protection schemes based on the carrier's requirement and actual networking scenario.

Procedure

- Configure a link aggregation group.

  Bind upstream ports 0/19/0 and 0/19/1 together as an aggregation link group. Each member port in the group transmits packets based on source MAC addresses. The working mode is LACP static aggregation.

  ```
  huawei(config)#link-aggregation 0/19 0-1 ingress workmode lacp-static
  ```

- Configure a protection group.

  Configure upstream ports 0/19/0 and 0/19/1 on board GIU as a port protection group. Set port 0/19/0 as the working port and port 0/19/1 as the protection port, set the working mode to time delay detection, and enable the protection group.

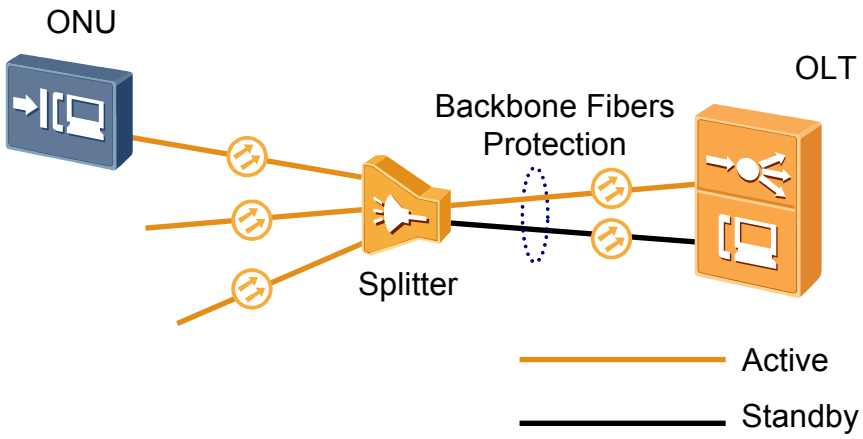
  ```
  huawei(config-protect)#protect-group first 0/19/0 second 0/19/1 eth workmode timedelay enable
  ```

- Configure the Type B protection.

  Figure 13-2 shows the Type B protection networking diagram.

Copyright © Huawei Technologies Co., Ltd.

Figure 13-2 Type B protection



Configure redundancy backup for ports 0/3/1 and 0/3/2 on the same GPON board on OLT. When port 0/3/1 fails, the system can automatically switch to port 0/3/2.

```
huawei(config)#protect-group 0 protect-target gpon-uni-port workmode timedelay
huawei(protect-group-0)#protect-group member port 0/3/1 role work
huawei(protect-group-0)#protect-group member port 0/3/2 role protect
huawei(protect-group-0)#protect-group enable
```

NOTE

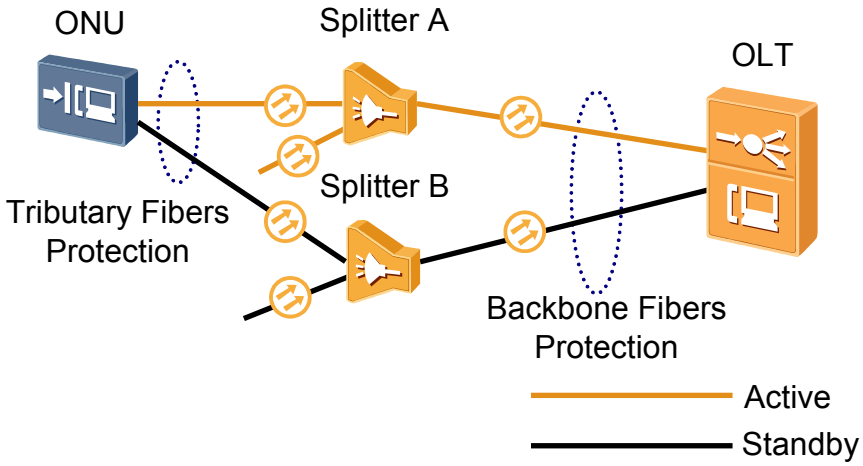
The configurations of services accessed by the ONUs remain the same after the Type B protection is configured. That is, the service configurations are applied only to the working GPON port.

- Configure the Type C single homing protection.

  Figure 13-3 shows networking diagram for the Type C single homing protection. Configure two 1:N optical splitters, one for connecting the working PON ports on the OLT and ONUs, and one for connecting the protection PON ports on the OLT and ONUs. This protection scheme protects both the backbone fibers and tributary fibers.

  The configurations of services accessed by the ONUs remain the same after the Type C single homing protection is configured. That is, the service configurations are applied only to the working PON port on the OLT and working upstream PON ports on the ONUs.

Figure 13-3 Type C single homing protection



Copyright © Huawei Technologies Co., Ltd.

As shown in the preceding figure, Type C single homing protecting is configured for optical fiber links between the OLT and ONU.

- The ports on the GPON service board are 0/3/1 and 0/3/2.
- The link at port 0/3/1 is the working link.
- The link at port 0/3/2 is the protection link.
- The ONU ID is 1.
- The ONU is authenticated by serial number (SN). The SN of the ONU is 32303131B39FD641 and the management mode is SNMP.
- The ID of the line profile bound to the ONU is 10.

```
huawei(config)#interface gpon 0/3
huawei(config-if-gpon-0/3)#ont add 1 1 sn-auth 32303131B39FD641 snmp ont-
lineprofile-id 10
huawei(config-if-gpon-0/3)#ont add 2 1 protect-side
huawei(config-if-gpon-0/3)#quit
huawei(config)#protect-group protect-target gpon-uni-ont workmode portstate
huawei(protect-group-1)#protect-group member port 0/3/1 ont 1 role work
huawei(protect-group-1)#protect-group member port 0/3/2 ont 1 role protect
huawei(protect-group-1)#protect-group enable
huawei(protect-group-1)#quit
```

- Configure the Type C dual homing protection.

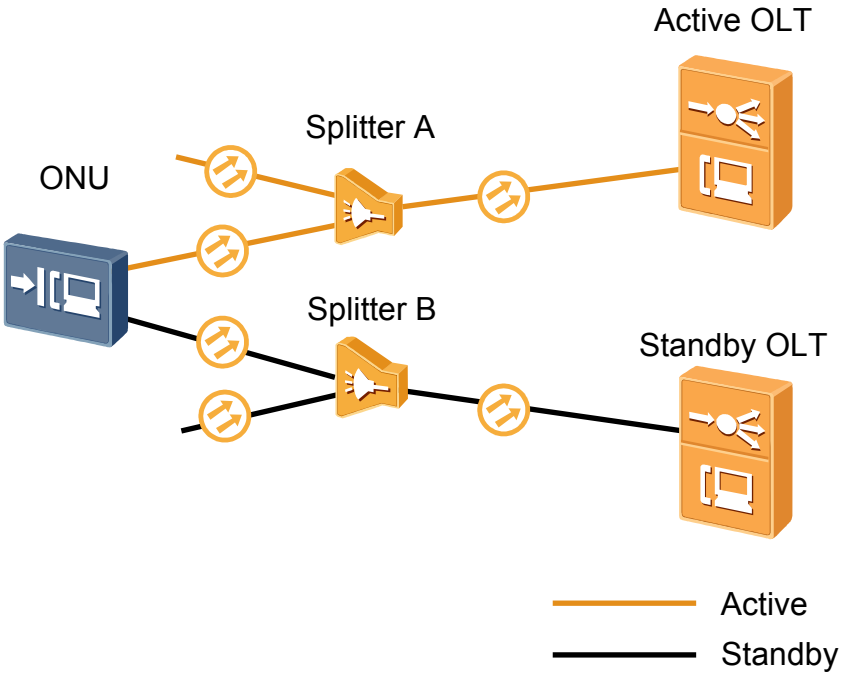
  Figure 13-4 shows the networking diagram for the Type C dual homing protection. Two PON ports on different OLTs, two PON ports on an ONU, two backbone optical fibers, two optical splitters, and two tributary optical fibers are configured to implement this protection. The difference between this protection scheme and the Type C single homing protection scheme is that the ONU needs to be dual homed to two OLTs in this protection scheme.

  The models and versions of main control boards on the active and standby OLTs must be the same. The models and versions of GPON boards on the active and standby OLTs also must be the same. Data on the active OLT cannot be automatically synchronized with that on the standby OLT. Therefore, data synchronization between the active and standby OLTs must be manually ensured.

  This protection scheme can be configured for only the Ethernet QinQ private line service. It does not support TDM services, including Native TDM and SAToP.

Copyright © Huawei Technologies Co., Ltd.

Figure 13-4 Type C dual homing protection



As shown in the preceding figure, Type C dual homing protection is configured for two OLTs (huawei_A and huawei_B).

- huawei_A is the active OLT while huawei_B is the standby OLT.
- The ports on the service boards on both OTLs are 0/3/1.
- The dual homing protection group ID is 1.
- The ONU ID is 1.
- The ONU is authenticated by serial number (SN). The SN of the ONU is 32303131B39FD641 and the management mode is SNMP.
- The ID of the line profile bound to the ONU is 10.

```
Configurations on the active OLT huawei_A:
huawei_A(config)#interface gpon 0/3
huawei_A(config-if-gpon-0/3)#ont add 1 1 sn-auth 32303131B39FD641 snmp ont-
lineprofile-id 10
huawei_A(config-if-gpon-0/3)#quit
huawei_A(config)#protect-group 1 protect-target gpon-uni-ont workmode dual-
parenting
huawei_A(protect-group-1)#protect-group member port 0/3/1 ont 1 role work
Configurations on the standby OLT huawei_B:
huawei_B(config)#interface gpon 0/3
huawei_B(config-if-gpon-0/3)#ont add 1 1 sn-auth 32303131B39FD641 snmp ont-
lineprofile-id 10
huawei_B(config-if-gpon-0/3)#quit
huawei_B(config)#protect-group 1 protect-target gpon-uni-ont workmode dual-
parenting
huawei_B(protect-group-1)#protect-group member port 0/3/1 ont 1 role protect
huawei_B(protect-group-1)#protect-group enable
```

----End

Copyright © Huawei Technologies Co., Ltd.

13.3.1.9 Verifying Services

This topic describes how to verify the Layer 2 interoperation service by checking the service configurations, service port status, and connectivity between PCs in different branches of an enterprise.

Prerequisites

PCs (with different MAC addresses) connected to different ONUs have been configured. Ensure that the IP addresses of the PCs are in the same network segment or subnet segment.

Procedure

Step 1 Check whether the VLAN configurations are correct.

```
huawei(config)#display vlan 300
{ <cr>|inner-vlan<K>|to<K> }:

  Command:
          display vlan 300
  VLAN ID: 300
  VLAN type: smart
  VLAN attribute: common
  VLAN description:
  VLAN forwarding mode in control board: VLAN-MAC
  VLAN forwarding mode: VLAN-MAC
  VLAN broadcast packet forwarding policy: forward
  VLAN unknown multicast packet forwarding policy: forward
  VLAN unknown unicast packet forwarding policy: forward
  VLAN bind service profile ID: 1
  VLAN bind RAIO profile index: -
  VLAN priority: -
  Standard port number: 0
  -------------------------------------------------------
  INDEX  TYPE  STATE F/ S/ P  VPI  VCI   FLOWTYPE FLOWPARA
  -------------------------------------------------------
     10  gpon  up    0/3 / 1  1    12    vlan     300
     11  gpon  up    0/3 / 1  2    12    vlan     300
  -------------------------------------------------------
  Service virtual port number: 2
  Note: F--Frame, S--Slot, P--Port,
        VPI indicates ONT ID for PON, VCI indicates GEM index for GPON,
        v/e--vlan/encap, pri-tag--priority-tagged
huawei(config)#display vlan service-profile profile-id 1

  Profile   ID: 1
  Profile Name: srvprof-1
  ------------------------------------------------------------------------
  Parameter                       Committed          Not Committed
  ------------------------------------------------------------------------
  Forwarding mode                 NotConfig          -
  Anti-macspoofing                NotConfig          -
  Anti-ipspoofing                 enable             -
  PPPoE MAC mode                  NotConfig          -
  BPDU tunnel                     enable             -
  RIP tunnel                      enable             -
  VTP-CDP tunnel                  enable             -
  DHCP mode                       n/a                -
  DHCP proxy                      enable             -
  DHCP option82                   enable             -
  PITP                            enable             -
  Broadcast packet policy         NotConfig          -
  Multicast packet policy         NotConfig          -
  Unknown unicast packet policy   NotConfig          -
```


Copyright © Huawei Technologies Co., Ltd.

```
  User-bridging                    enable           -
  IPoE VMAC                        NotConfig        -
  PPPoE VMAC                       NotConfig        -
  PPPoA VMAC                       NotConfig        -
  Mismatch IGMP packet policy      discard          -
  VMAC aging mode                  MAC-learning     -
  OSPF tunnel                      enable           -
  Layer-3 protocol tunnel          enable           -
  MAC-address learning fabric      enable           -
  DHCPv6 mode                      n/a              -
  DHCPv6 option                    enable           -
  PPPoA MAC mode                   NotConfig        -
  Anti-IPv6spoofing                enable           -
  IPv6 DAD proxy                   disable          -
  Bind route and ND                disable          -
  NS-reply function                disable          -
  ARP-reply function               disable          -
  DHCP relay-interface relay-agent NotConfig        -
  Multicast packet policy fabric   forward          -
  ------------------------------------------------------------------------
  Binding VLAN list            : 300
  ------------------------------------------------------------------------
```

Step 2 Check whether the service port is normal.

```
huawei(config)#display service-port vlan 300
{ <cr>|autosense<K>|sort-by<K> }:

  Command:
          display service-port vlan 300
  Switch-Oriented Flow List
  ---------------------------------------------------------------------------
  INDEX VLAN VLAN     PORT F/ S/ P VPI  VCI   FLOW  FLOW       RX   TX   STATE
        ID   ATTR     TYPE                    TYPE  PARA
  ---------------------------------------------------------------------------
     10  300 common   gpon 0/3 /1  1    12    vlan  300        -    -    up
     11  300 common   gpon 0/3 /1  2    12    vlan  300        -    -    up
  ---------------------------------------------------------------------------
   Total : 2  (Up/Down :    2/0)
huawei(config)#display statistics service-port 10
 Number of upstream bytes             : 1044794
 Number of upstream packets           : 4522
 Number of upstream discard packets   : 200
 Number of downstream bytes           : 1351261
 Number of downstream packets         : 4677
 Number of downstream discard packets : 0
```

Step 3 Check the connectivity between the PCs.

1. Use the PCs to ping each other. If the PCs can ping each other successfully, the PCs are reachable to each other.

   For example, the IP addresses of PC1 and PC2 are 192.168.1.10 and 192.168.1.30 respectively. Ping PC2 on PC1. The expected result is as follows:

Copyright © Huawei Technologies Co., Ltd.

```
C:\>ping 192.168.1.30

Pinging 192.168.1.30 with 32 bytes of data:

Reply from 192.168.1.30: bytes=32 time=3ms TTL=128
Reply from 192.168.1.30: bytes=32 time=2ms TTL=128
Reply from 192.168.1.30: bytes=32 time=2ms TTL=128
Reply from 192.168.1.30: bytes=32 time=2ms TTL=128

Ping statistics for 192.168.1.30:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 3ms, Average = 2ms
```

2. You can see one PC in **My Network Places** on the other PC and the two PCs can share data.

----End

13.3.2 Enterprise DDN Private Line Access Service

Enterprise DDN private line service is converted to E1 signals. ONUs access the E1 signals and transmit them in Native TDM mode.

13.3.2.1 Service Requirement and Application Scenario

Service Requirement

The DDN private line service is widely used in financial departments, governments, and enterprises that require highly real-time data switching. It provides a rate from 64 kbit/s to 2 Mbit/s. GPON access in OLT+ONU mode can access the DDN private line service along with other data services and voice service. This access mode does not require independent maintenance of the DDN network, simplifying network architecture.

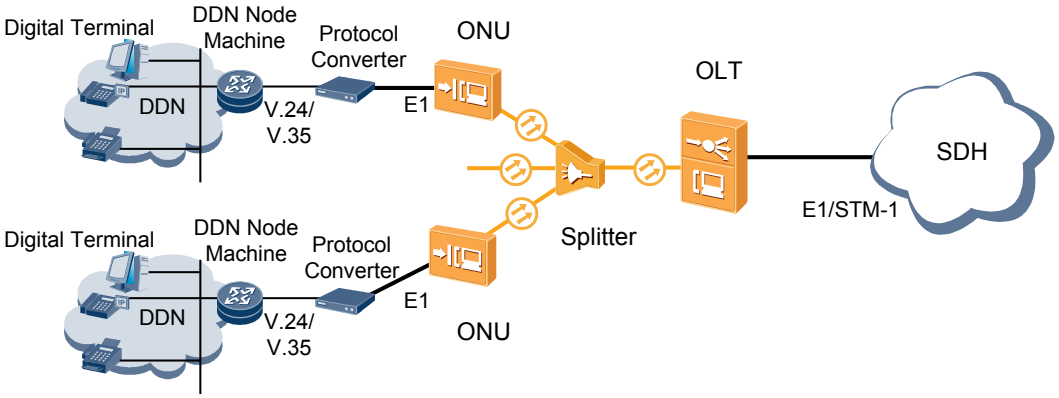
Application Scenario

As shown in **Figure 13-5**, a protocol converter is deployed between an ONU and DDN node machine to convert DDN private line services to E1 services. The ONU accesses the E1 services and encapsulates the service packets in TDM over GEM mode and then transmits the packets to the OLT. The OLT decapsulates the service packets to E1 data and transmits the data to the SDH network through upstream E1/STM-1 ports, achieving transparent transmission of DDN services.

Applicable ONUs: MA5612, MA5628, MA5616

Copyright © Huawei Technologies Co., Ltd.

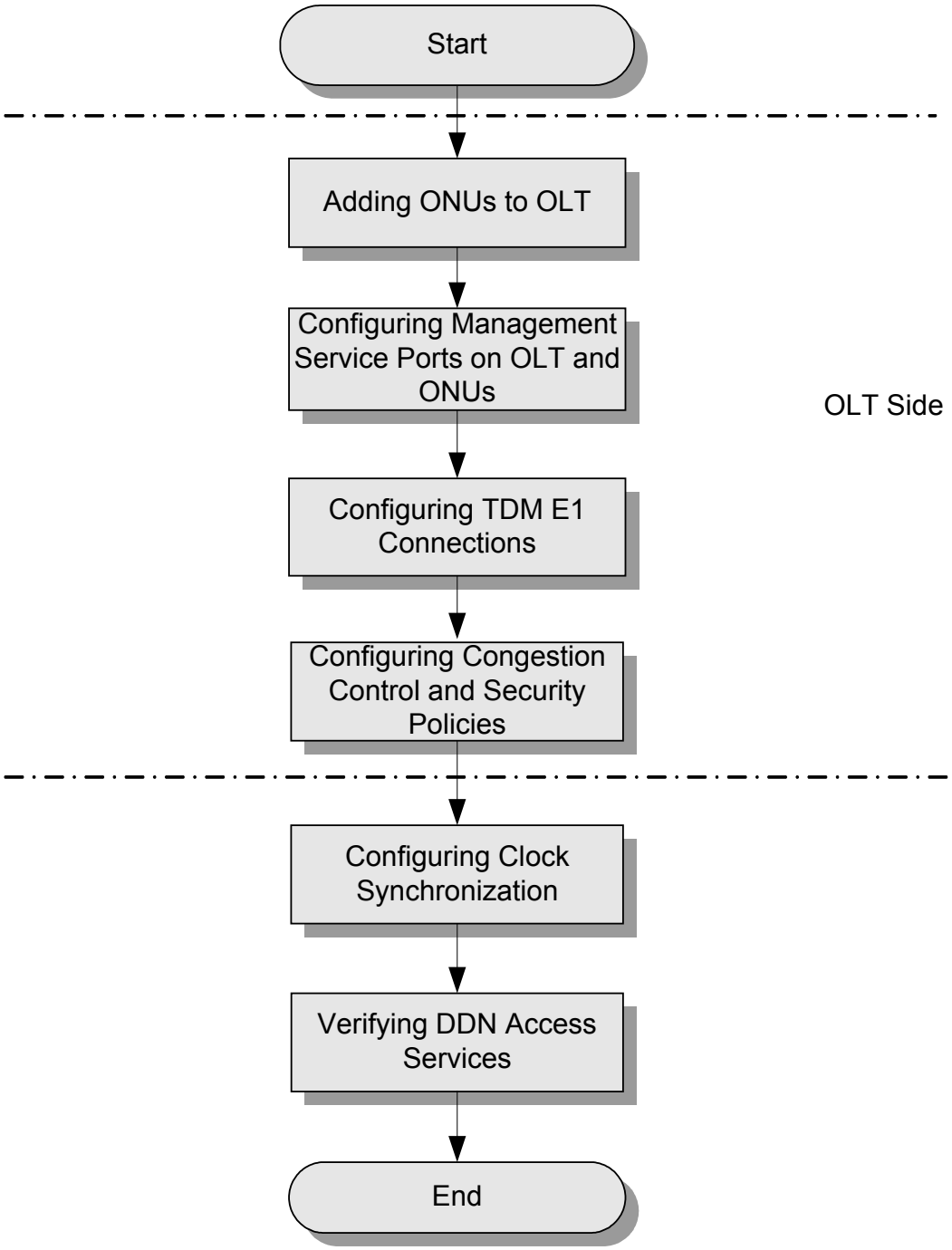
Figure 13-5 Networking diagram of the DDN private line access service



13.3.2.2 Configuration Process

The following figure shows the configuration process for the DDN private line access service.

Copyright © Huawei Technologies Co., Ltd.



13.3.2.3 Adding ONUs to OLT

This topic describes how to add ONUs to the OLT. ONUs can be configured only after they are added to the OLT successfully.

Context

- When adding ONUs, you need to bind related profiles to the ONUs, including the DBA profile, line profile, and alarm profile.

Copyright © Huawei Technologies Co., Ltd.

- An ONU can be added in two modes: offline addition and online confirmation. Select either mode as required.

Data Plan

Table 13-4 Key data plan

Configuration Item	Data
DBA profile	DBA profile for management service: dba-profile_1 (system default) DBA profile for private line service: ● Profile ID: 21 ● Profile type: Fixed bandwidth and minimum delay ● DBA bandwidth: 28928 kbit/s (Each ONU accesses four E1 private lines and each line has a recommended DBA bandwidth of 7232 kbit/s.)
Line profile	Profile ID: 11 T-CONT ID: 1 (for private line service) and 2 (for management service) GEM port ID for management service: 11 GEM port ID for DDN private line service: 13
Networking data	PON port: 0/3/1 ONU parameters: ● ONU ID: 1 ● SN: 32303131B39FD641

Procedure

Step 1 Configure GPON ONU profiles.

1. Configure a DBA profile. Enable the bandwidth compensation function and set the DBA bandwidth allocation mode for the GPON port to minimum bandwidth delay.

```
huawei(config)#dba-profile add profile-id 21 type1 fix 28928
bandwidth_compensate yes
huawei(config)#interface gpon 0/3
huawei(config-if-gpon-0/3)#port dba bandwidth-assignment-mode 1 min-loop-delay
huawei(config-if-gpon-0/3)#quit
```

2. Configure an ONU line profile.

```
huawei(config)#ont-lineprofile gpon profile-id 11
huawei(config-gpon-lineprofile-11)#tcont 1 dba-profile-id 21  //Bind T-CONT 1
to DBA profile 21
huawei(config-gpon-lineprofile-11)#tcont 2 dba-profile-id 1  //Bind T-CONT 2
to DBA profile 1
huawei(config-gpon-lineprofile-11)#gem add 11 eth tcont 2
huawei(config-gpon-lineprofile-11)#gem add 13 tdm tcont 1 //Add GEM port 13 to
T-CONT 1.
huawei(config-gpon-lineprofile-11)#gem mapping 11 0 vlan 8
huawei(config-gpon-lineprofile-11)#gem mapping 13 1 e1 1 //Map GEM port 13 to
E1 port 1 on the ONU.
```


Copyright © Huawei Technologies Co., Ltd.

```
huawei(config-gpon-lineprofile-11)#commit
huawei(config-gpon-lineprofile-11)#quit
```

3. (Optional) Configure an alarm profile.
   - The default GPON alarm profile ID is 1. The value of each alarm threshold is **0** which indicates that alarms are not reported.
   - In this example, the default alarm profile is used and no configuration is required.

Step 2 Add ONUs to the OLT.

1. Add ONU 3 in offline mode.

```
huawei(config)#interface gpon 0/3
huawei(config-if-gpon-0/3)#ont add 1 ontid 1 sn-auth 32303131B39FD641
snmp ont-lineprofile-id 11
```

2. (Optional) Bind an alarm profile.

   By default, an ONU will be automatically bound to alarm profile 1 (default profile). You need to manually bind an alarm profile to an ONU only when the default alarm profile does not meet requirements.

   In this example, the default alarm profile is used. Therefore, you do not need to manually bind an alarm profile.

Step 3 Confirm the ONU status.

After adding an ONU, run the **display ont info** command to query the current status of the ONU. Ensure that **Control flag** is **active**, **Run State** is **online**, and **Config state** is **normal**.

The following uses ONU 1 as an example to describe how to confirm ONU status.

```
huawei(config-if-gpon-0/3)#display ont info 1 1
  ------------------------------------------------------------------------
  F/S/P                : 0/3/1
  ONT-ID               : 1
  Control flag         : active    //Indicates that the ONU is
activated.
  Run state            : online    //Indicates that the ONU is
online.
  Config state         : normal    //Indicates that the ONU is in normal
state.
...//Other command output is omitted.
huawei(config-if-gpon-0/3)#quit
```

----End

Follow-up Procedure

When **Config state** is **failed**, **Run state** is **offline**, or **Match state** is **mismatch**:

- If **Control flag** is **deactive**, run the **ont active** command in GPON mode to activate the ONU.
- If **Run state** is **offline**, a physical line may be broken or the optical module may be damaged. Check the line and the optical module.
- If **Config state** is **failed**, the configured ONU capability exceeds the actual ONU capability. In this case, run the **display ont failed-configuration** command in the diagnose mode to check the failed configuration item and the failure cause. Then, rectify the fault accordingly.
- If the ONU does not match, that is, **Match state** is **mismatch**, the port types and number of ports undermatch the actual port types and number of ports supported by the ONU. In this case, run the **display ont capability** command to query the actual capability of the ONU, and then select one of the following modes to modify the ONU configuration:

Copyright © Huawei Technologies Co., Ltd.

- Create a proper ONU profile according to the actual capability of the ONU, and then run the **ont modify** command to modify the configuration data of the ONU.
- Modify the ONU profile according to the actual capability of the ONU and save the modification. Then, the ONU automatically recovers the configuration successfully.

13.3.2.4 Configuring Management Service Ports on OLT and ONUs

This topic describes how to configure management service ports (also called service flows) on the OLT and ONUs. After the connections between the in-band management service ports on the OLT and ONUs are reachable, you can log in to the ONUs on the OLT and configure the ONUs.

Data Plan

Configuration Item	Data
Management VLAN and management IP address for OLT	Management VLAN ID: 8 Management VLAN type: smart In-band management IP address: 192.168.50.1/24
Management VLAN and management IP address for ONU	Management VLAN ID: 8 Management VLAN type: smart In-band management IP address for ONU 3: 192.168.50.2/24

Procedure

Step 1 Configure the in-band management VLAN and IP address for the OLT.

Set the in-band management VLAN to 8, VLAN priority to 6, and IP address to 192.168.50.1/24.

```
huawei(config)#vlan 8 smart
huawei(config)#port vlan 8 0/19 0
huawei(config)#vlan priority 8 6
huawei(config)#interface vlanif 8
huawei(config-if-vlanif8)#ip address 192.168.50.1 24
huawei(config-if-vlanif8)#quit
```

Step 2 Configure the in-band management VLAN and IP address for the ONU.

```
huawei(config)#interface gpon 0/3
huawei(config-if-gpon-0/3)#ont ipconfig 1 1 static ip-address 192.168.50.2 mask
255.255.255.0 gateway
192.168.50.1 vlan 8
huawei(config-if-gpon-0/3)#quit
```

Step 3 Configure the in-band management service port.

Set the management VLAN to 8, GEM port ID to 11, and user VLAN to 8. The OLT does not rate limit the in-band management service port. Therefore, directly use the default traffic profile 6.

Copyright © Huawei Technologies Co., Ltd.

```
huawei(config)#service-port vlan 8 gpon 0/3/1 ont 1 gemport 11 multi-service
user-vlan 8 rx-cttr 6 tx-cttr 6
```

Step 4 Confirm that the connection between the management service ports on the OLT and ONU is reachable.

- Run the **ping *ONU ip*** command on the OLT to verify the connectivity between the OLT and ONU. If the OLT receives ICMP ECHO-REPLY packets from the ONU, the connection is reachable.
- When the connection is reachable, you can remote log in to the ONU from the OLT and configure the ONU.

----End

13.3.2.5 Configuring TDM Connections

This topic describes how to configure Native TDM connections between GPON ports and E1/STM-1 upstream ports to transmit E1/STM-1 private line service data.

Prerequisites

Required hardware is available:

- TOPA+NH1A for upstream transmission through E1
- TOPA+O2CE for upstream transmission through STM-1
- GPON board: GPBC, GPBD

Context

The OLT can transmit data to the SDH network through E1 or STM-1 lines. Each E1 line provides 2 Mbit/s bandwidth. After being mapped, aligned, and encapsulated, 63xE1 signals are multiplexed into one STM-1 signal through VC12. One STM-1 line provides 155 Mbit/s.

When the OLT transmits data to SDH equipment through STM-1 lines, pay attention to the VC12 mode and VC12 number.

- When the OLT is interconnected with Huawei SDH equipment, the VC12 mode is huawei and the VC12 numbers on the OLT and the SDH equipment must be consistent.
- When the OLT is interconnected with Lucent SDH equipment, the VC12 mode is lucent. The VC12 numbers has the following mapping relationships (which can be queried using the **display vc12-mode-table** command):

  Huawei: Mapping between the multiplexing number and VC12 number: VC12 number = (TUG3–1) + (TUG2–1) x 3 + (TU12–1) x 21

  Lucent: Mapping between the multiplexing number and VC12 number: VC12 number = (TU12–1) + (TUG2–1) x 3 + (TUG3–1) x 21

Copyright © Huawei Technologies Co., Ltd.

Data Plan

Upstream Transmission Mode	Data
Upstream transmission through E1	Port on the TOPA board: 0/5/0 Daughter board type: NH1A (provides E1 ports)
Upstream transmission through STM-1	Port on the TOPA board: 0/5/0 Daughter board type: O2CE (provides STM-1 ports) VC12 number: 0 **NOTE** The VC12 parameter must match that on the interconnected SDH equipment. Otherwise, services fail.

Procedure

- Configure a TDM E1 connection for E1 upstream transmission.

  ```
  huawei(config)#tdm-connect connectid 1 tdm 0/5/0 gpon 0/3/1 ontid 3 gemportIndex 13
  ```

- Configure a TDM E1 connection for STM-1 upstream transmission.

  ```
  huawei(config)#tdm-connect connectid 1 tdm 0/5/0 vc12 0 gpon 0/3/1 ontid 3 gemportIndex 13
  ```

----End

13.3.2.6 Configuring Clock Synchronization

In this scenario, the E1/STM-1 line clock can be used to achieve network-wide clock synchronization.

Prerequisites

The clock daughter board CKMC/CKMD must be on the SCU main control board.

Context

Configuration roadmap for clock synchronization:

1. The OLT traces the upstream E1/STM-1 line clock of the TOPA board as the system clock.
2. The system clock is delivered to an ONU through optical paths of the GPON board.
3. The ONU uses the line clock of the GPON upstream port as the system clock.
4. The ONU E1 transmit clock is synchronized with the system clock of the ONU.

Procedure

- **Configure a clock on the OLT.**
  1. Add a system clock source.

Copyright © Huawei Technologies Co., Ltd.

Run the **clock source** command to configure the line clock of E1/STM-1 port 0/5/0 on the TOPA board as the system clock source. Set the ID of the clock source to 0.

The clock module automatically judges the type of the specified clock source (E1/STM-1) and selects a reference source for phase lock based on priorities.

```
huawei(config)#clock source 0 0/5/0
```

2. Configure a priority for the system clock source.

   Run the **clock priority** command to set the priority of clock source 0 to the highest priority.

```
huawei(config)#clock priority system 0
```

3. Query configurations and the status of the system clock source.

   Run the **display clock source system** command to query configurations and the status of the clock source. Ensure that configurations of the system clock source are correct and the status is **Normal**.

```
huawei(config)#display clock source system

-------------------------------------------------------------------------
-----
  Index  Board    Source   Clk-type  State       Priority QL
Selected

-------------------------------------------------------------------------
-----
    0    H801TOPA 0/5/0    E1        Normal      0        ---
YES

-------------------------------------------------------------------------
-----
```

   Run the **display clock mode** command to query the clock working mode. Ensure that the clock daughter board works in tracing mode.

```
huawei(config)#display clock mode
  Clock manage-mode:Third-mode
  Clock subboard work-mode:Tracing
```

- **Configure a clock on the ONU.**

1. Configure the GPON line clock as the system clock.

   The system clock of the OLT is delivered to the ONU through the GPON port on the OLT, achieving clock synchronization between the OLT and the ONU.

   a. Run the **clock source** command to configure the clock recovered from the GPON upstream port as the system clock of the ONU.

   b. Run the **clock priority** command to configure the priority of the clock source.

```
huawei(config)#clock source 0 0/0/1
  Clock source set succeeded

huawei(config)#clock priority system 0
```

2. Configure the system clock as the transmit clock for an E1 port.

   a. Run the **interface tdm** command to enter the E1 port configuration mode.

   b. Run the **tx clock** or **port** *portid* **udt system** command to configure the system clock as the transmit clock of the port.

   c. Run the **display port state** command to query the transmit clock of the E1 port.

```
huawei(config)#interface tdm
huawei(config-if-tdm-)#port 0 udt system
```


Copyright © Huawei Technologies Co., Ltd.

```
huawei(config-if-tdm-)#display port state 0
  ---------------------------------------
  Port           : 0
  State          : normal
  Mode           : UDT
  Code           : HDB3
  Looptype       : -
  Timeslot       : -
  Clock          : system
  CRC4           : -
  Signaling      : -
  ESF            : -
  Impedance      : 120 Ohm
  ---------------------------------------
```

3. Query configurations and the status of the system clock source.

   Run the **display clock source** command to query configurations and the status of the system clock source.

```
huawei(config-if-tdm-)#quit
huawei(config)#display clock source
  ------------------------------------------------------------------
  Index  Config   Type   Source      State     Priority   Output
  ------------------------------------------------------------------
    0    YES      line   0/0/1       Normal    0          YES
    1    NO       --     -/ -/ -     ---       ---        ---
    2    NO       --     -/ -/ -     ---       ---        ---
    3    NO       --     -/ -/ -     ---       ---        ---
    4    NO       --     -/ -/ -     ---       ---        ---
    5    NO       --     -/ -/ -     ---       ---        ---
    6    NO       --     -/ -/ -     ---       ---        ---
    7    NO       --     -/ -/ -     ---       ---        ---
    8    NO       --     -/ -/ -     ---       ---        ---
    9    NO       --     -/ -/ -     ---       ---        ---
  ------------------------------------------------------------------
```

----End

13.3.2.7 Verifying Services

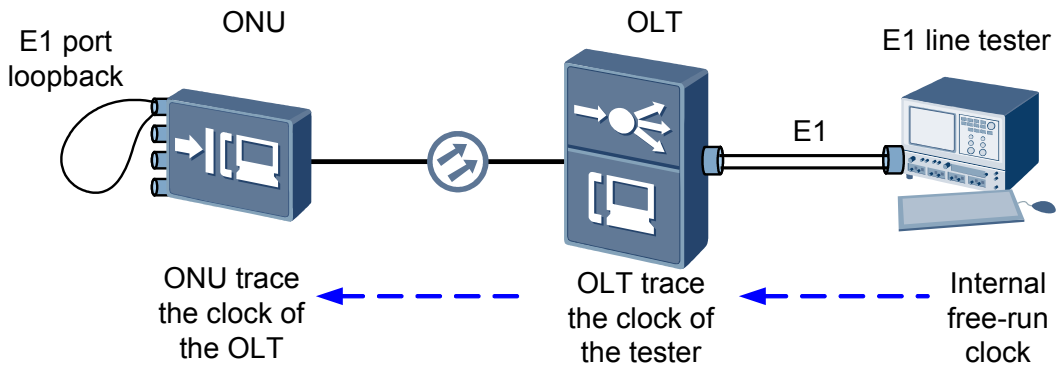
This topic describes how to use the PDH/SDH tester to verify the private line access service.

Prerequisites

The private line service has been configured.

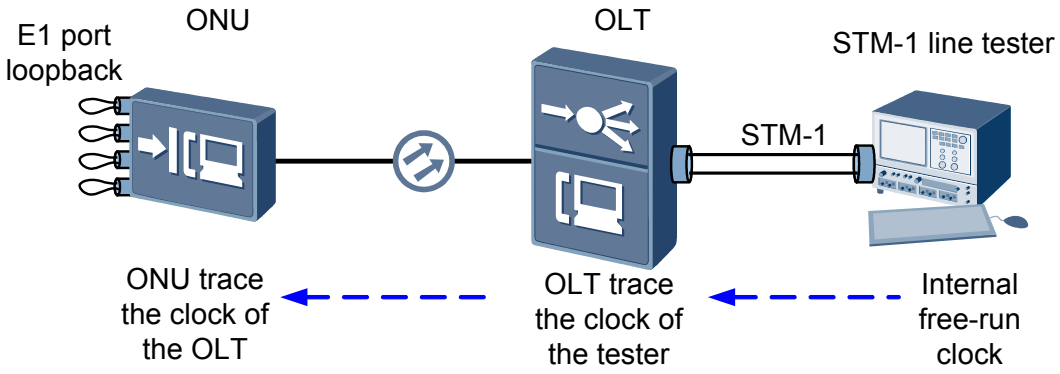
Networking

Figure 13-6 Test setup for E1 upstream service



Copyright © Huawei Technologies Co., Ltd.

Figure 13-7 Test setup for STM-1 upstream service



Procedure

Step 1 Set up network environment according to the preceding diagrams for service acceptance tests.

NOTE

Ensure clock synchronization for the test. It is recommended that the tester use the internal free-run clock, the OLT trace the clock of the tester, and the ONU trace the clock of the OLT.

Step 2 Use the E1 or STM-1 line tester to send packets for the test.

The test duration must be 12 hours or longer. There should be no alarms on the tester and the bit error rate must be less than 1E-9.

----End

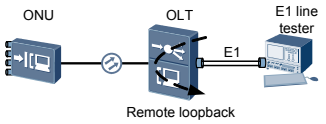
Follow-up Procedure

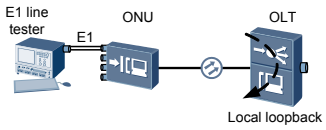
When the test on service connectivity fails, you can check for the failure causes by performing loopbacks. The following loopbacks are supported:

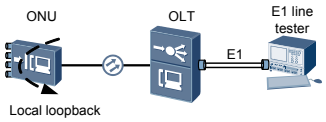
- Remote loopback on the OLT TOPA board
- Local loopback on the OLT TOPA board
- Local loopback on the ONU
- Remote loopback on the ONU

Copyright © Huawei Technologies Co., Ltd.

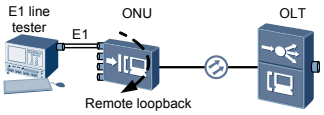
Loopback Mode	Function	Networking	Configuration

Remote loopback on the TOPA board	Loops back signals to the network side on the TOPA board on the OLT. This loopback checks whether the service from the TOPA board to the network-side channel is normal.		Enable/Disable the remote loopback for the E1 port.
			`huawei(config)#interface top 0/5`
			`huawei(config-if-top-0/5)#loopback 0 remote`
			`huawei(config-if-top-0/5)#undo loopback 0`
			Enable/Disable the remote loopback for the STM-1 port.
			`huawei(config)#interface top-stm1 0/5`
			`huawei(config-if-top-stm1-0/5)#loopback 0 remote`
			`huawei(config-if-top-stm1-0/5)#undo loopback 0`

Local loopback on the TOPA board	Loops back signals to the user side on the TOPA board on the OLT. This loopback checks whether the link between the TOPA board and the E1 port on the ONU is normal.		Enable/Disable the local loopback for the E1 port.
			`huawei(config)#interface top 0/5`
			`huawei(config-if-top-0/5)#loopback 0 local`
			`huawei(config-if-top-0/5)#undo loopback 0`
			Enable/Disable the local loopback for the STM-1 port.
			`huawei(config)#interface top-stm1 0/5`
			`huawei(config-if-top-stm1-0/5)#loopback 0 local`
			`huawei(config-if-top-stm1-0/5)#undo loopback 0`

Local loopback on the ONU	Loops back signals to the network side on the ONU. This loopback checks whether the link between the E1 port on the ONU and the TOPA board on the OLT is normal.		`huawei(config)#interface tdm`
			`huawei(config-if-tdm-)#loopback 0 local`
			`huawei(config-if-tdm-)#undo loopback 0`

Copyright © Huawei Technologies Co., Ltd.

Loopback Mode	Function	Networking	Configuration
Remote loopback on the ONU	Loops back signals to the user side on the ONU. This loopback checks whether the link between the ONU and user terminal is normal.		huawei(config)#**interface tdm** huawei(config-if-tdm-)#**loopback 0 remote** huawei(config-if-tdm-)#**undo loopback 0**

13.3.3 Enterprise IP PBX Private Line Access Service

ONUs provide GE/FE ports to access IP private branch exchange (PBX) services of an enterprise and transmit them to an OLT. Then, the OLT forwards the service data upstream to the packet switched network (PSN). This achieves unified carrying of voice, data, and video services.

13.3.3.1 Service Requirement and Application Scenario

Service Requirement

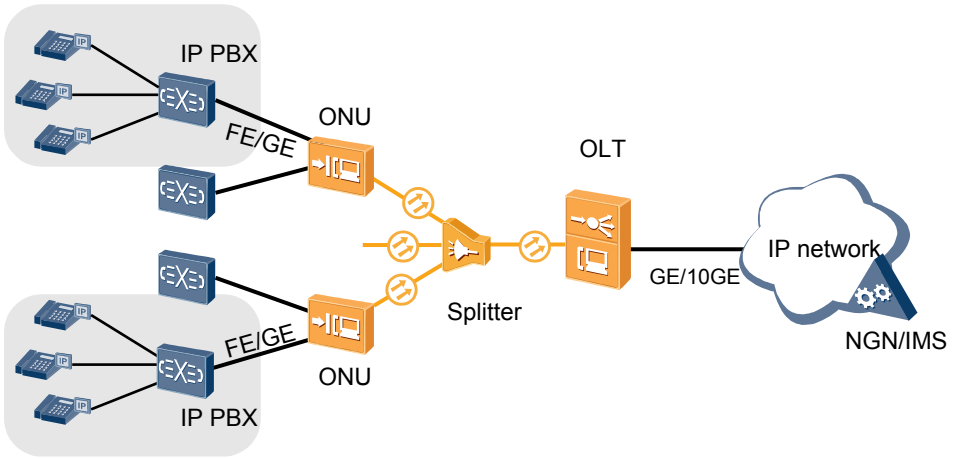
- The IP private branch exchange (PBX) data can be transparently transmitted on the PON network.
- The operation method for end users connected to the IP PBX is not changed.

Application Scenario

As shown in **Figure 13-8**, ONUs access IP PBX services through FE/GE ports. The OLT transparently transmits the data to the IP network in QinQ mode.

Applicable ONUs: MA5612, MA5628, MA5616

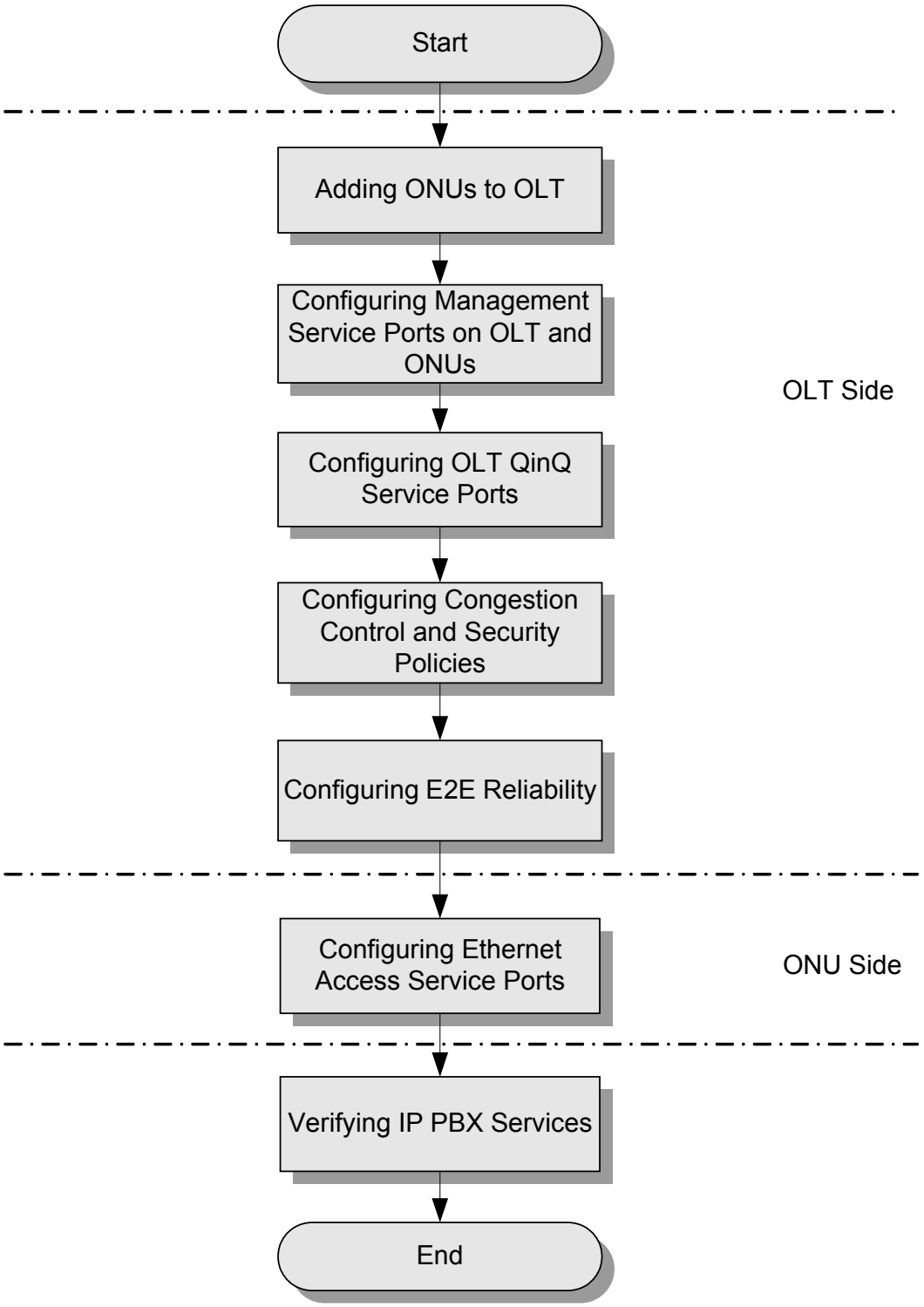
Figure 13-8 Networking diagram of the IP PBX access service



Copyright © Huawei Technologies Co., Ltd.

13.3.3.2 Configuration Process

The following figure shows the configuration process for the IP PBX access service.



Copyright © Huawei Technologies Co., Ltd.

13.3.3.3 Adding ONUs to OLT

This topic describes how to add ONUs to the OLT. ONUs can be configured only after they are added to the OLT successfully.

Context

- When adding ONUs, you need to bind related profiles to the ONUs, including the DBA profile, line profile, and alarm profile.
- An ONU can be added in two modes: offline addition and online confirmation. Select either mode as required.

Data Planning

Table 13-5 Key data plan

Configuration Item	Data
DBA profile	Profile ID: 20 Profile type: Type 3 Assured bandwidth: 100 Mbit/s Maximum bandwidth: 120 Mbit/s
Line profile	Profile ID: 10 T-CONT ID: 4 GEM port ID for management service: 11 GEM port ID for other services: 12
Networking data	PON port: 0/3/1 ONU parameters: ● ONU ID: 1 ● SN: 32303131B39FD641

Procedure

Step 1 Configure GPON ONU profiles.

1. Configure a DBA profile.

```
huawei(config)#dba-profile add profile-id 20 type3 assure 102400 max 122880
```

2. Configure an ONU line profile.

```
huawei(config)#ont-lineprofile gpon profile-id 10
huawei(config-gpon-lineprofile-10)#tcont 4 dba-profile-id 20  //Bind T-CONT 4
to DBA profile 20
huawei(config-gpon-lineprofile-10)#gem add 11 eth tcont 0
huawei(config-gpon-lineprofile-10)#gem add 12 eth tcont 4 //Add GEM port 12 to
T-CONT 4
huawei(config-gpon-lineprofile-10)#gem mapping 11 0 vlan 8
huawei(config-gpon-lineprofile-10)#gem mapping 12 1 vlan 300 //Map GEM port 12
to CVLAN 300
```


Copyright © Huawei Technologies Co., Ltd.

```
huawei(config-gpon-lineprofile-10)#commit
huawei(config-gpon-lineprofile-10)#quit
```

3. (Optional) Configure an alarm profile.
   - The default GPON alarm profile ID is 1. The value of each alarm threshold is **0** which indicates that alarms are not reported.
   - In this example, the default alarm profile is used and no configuration is required.

Step 2 Add ONUs to the OLT.

1. Add ONU 1 in offline mode.

```
huawei(config)#interface gpon 0/3
huawei(config-if-gpon-0/3)#ont add 1 ontid 1 sn-auth 32303131B39FD641
snmp ont-lineprofile-id 10
```

2. (Optional) Bind an alarm profile.

   By default, an ONU will be automatically bound to alarm profile 1 (default profile). You need to manually bind an alarm profile to an ONU only when the default alarm profile does not meet requirements.

   In this example, the default alarm profile is used. Therefore, you do not need to manually bind an alarm profile.

Step 3 Confirm the ONU status.

After adding an ONU, run the **display ont info** command to query the current status of the ONU. Ensure that **Control flag** is **active**, **Run State** is **online**, and **Config state** is **normal**.

The following uses ONU 1 as an example to describe how to confirm ONU status.

```
huawei(config-if-gpon-0/3)#display ont info 1 1
  ------------------------------------------------------------------------
  F/S/P                : 0/3/1
  ONT-ID               : 1
  Control flag         : active    //Indicates that the ONU is
activated.
  Run state            : online    //Indicates that the ONU is
online.
  Config state         : normal    //Indicates that the ONU is in normal
state.
...//Other command output is omitted.
huawei(config-if-gpon-0/3)#quit
```

----End

Follow-up Procedure

When **Config state** is **failed**, **Run state** is **offline**, or **Match state** is **mismatch**:

- If **Control flag** is **deactive**, run the **ont active** command in GPON mode to activate the ONU.
- If **Run state** is **offline**, a physical line may be broken or the optical module may be damaged. Check the line and the optical module.
- If **Config state** is **failed**, the configured ONU capability exceeds the actual ONU capability. In this case, run the **display ont failed-configuration** command in the diagnose mode to check the failed configuration item and the failure cause. Then, rectify the fault accordingly.
- If the ONU does not match, that is, **Match state** is **mismatch**, the port types and number of ports undermatch the actual port types and number of ports supported by the ONU. In this case, run the **display ont capability** command to query the actual capability of the ONU, and then select one of the following modes to modify the ONU configuration:

Copyright © Huawei Technologies Co., Ltd.

- Create a proper ONU profile according to the actual capability of the ONU, and then run the **ont modify** command to modify the configuration data of the ONU.
- Modify the ONU profile according to the actual capability of the ONU and save the modification. Then, the ONU automatically recovers the configuration successfully.

13.3.3.4 Configuring Management Service Ports on OLT and ONUs

This topic describes how to configure management service ports (also called service flows) on the OLT and ONUs. After the connections between the in-band management service ports on the OLT and ONUs are reachable, you can log in to the ONUs on the OLT and configure the ONUs.

Data Plan

Configuration Item	Data
Management VLAN and management IP address for OLT	Management VLAN ID: 8 Management VLAN type: smart In-band management IP address: 192.168.50.1/24
Management VLAN and management IP address for ONU	Management VLAN ID: 8 Management VLAN type: smart In-band management IP address for ONU 3: 192.168.50.2/24

Procedure

Step 1 Configure the in-band management VLAN and IP address for the OLT.

Set the in-band management VLAN to 8, VLAN priority to 6, and IP address to 192.168.50.1/24.

```
huawei(config)#vlan 8 smart
huawei(config)#port vlan 8 0/19 0
huawei(config)#vlan priority 8 6
huawei(config)#interface vlanif 8
huawei(config-if-vlanif8)#ip address 192.168.50.1 24
huawei(config-if-vlanif8)#quit
```

Step 2 Configure the in-band management VLAN and IP address for the ONU.

```
huawei(config)#interface gpon 0/3
huawei(config-if-gpon-0/3)#ont ipconfig 1 1 static ip-address 192.168.50.2 mask
255.255.255.0 gateway
192.168.50.1 vlan 8
huawei(config-if-gpon-0/3)#quit
```

Step 3 Configure the in-band management service port.

Set the management VLAN to 8, GEM port ID to 11, and user VLAN to 8. The OLT does not rate limit the in-band management service port. Therefore, directly use the default traffic profile 6.

Copyright © Huawei Technologies Co., Ltd.

```
huawei(config)#service-port vlan 8 gpon 0/3/1 ont 1 gemport 11 multi-service
user-vlan 8 rx-cttr 6 tx-cttr 6
```

Step 4 Confirm that the connection between the management service ports on the OLT and ONU is reachable.

- Run the **ping *ONU ip*** command on the OLT to verify the connectivity between the OLT and ONU. If the OLT receives ICMP ECHO-REPLY packets from the ONU, the connection is reachable.
- When the connection is reachable, you can remote log in to the ONU from the OLT and configure the ONU.

----End

13.3.3.5 Configuring OLT QinQ Service Ports

This topic describes how to configure QinQ service ports on the OLT to add an SVLAN tag to IP PBX packets sent from ONUs and transmit the packets to the upper-layer IP network.

Data Plan

Configuration Item	Data
SVLAN	VLAN ID: 1300 VLAN attribute: q-in-q
CVLAN (upstream VALN of the ONU)	300
Traffic profile	Profile ID: 10 Assured bandwidth: 100 Mbit/s Priority source: user-cos Default priority: 4

NOTE

Because packets transmitted from the OLT carry two VLAN tags, the interconnected equipment on the metro network must be able to identify and restore packets with two VLAN tags.

Procedure

Step 1 Configure an SVLAN and add an upstream port to it.

Set the SVLAN ID of the IP PBX service to 1300, VLAN type to smart, VLAN attribute to QinQ, and add upstream port 0/19/0 to the VLAN.

```
huawei(config)#vlan 1300 smart
huawei(config)#vlan attrib 1300 q-in-q
huawei(config)#port vlan 1300 0/19 0
```

Step 2 Configure a traffic profile for the service port.

Copyright © Huawei Technologies Co., Ltd.

Add a new traffic profile 10 and set the assured rate to 100 Mbit/s. Packets transmitted upstream use the priority (4 by default) copied from the user side. Packets transmitted downstream use the priority carried by themselves.

```
huawei(config)#traffic table ip index 10 cir 102400 priority user-cos 4 priority-policy tag-in-package
```

Step 3 Configure a QinQ service port.

According to **13.2.2 Principle of VLAN Data Plan**, VLANs of packets sent from the IP PBX are all translated to CLVAN 300. Then, the OLT adds an SVLAN tag to the packets: CVLAN<->SVLAN+CVLAN. Traffic profile 10 is used.

```
huawei(config)#service-port vlan 1300 gpon 0/3/1 ont 1 gemport 12 multi-service user-vlan 300 rx-cttr 10 tx-cttr 10
```

NOTE

If you need to transparently transmit the CVLAN to SVLAN, then user qinq SVLAN, set SVLAN=CVLAN, and creat a service-port with "tag-transform transparent".

----End

13.3.3.6 Configuring Ethernet Access Service Ports on ONUs

This topic describes how to configure service ports on ONUs and upstream VLANs to make the connections between ONUs and user terminals reachable and create upstream channels between ONUs and the OLT, achieving access of IP PBX services through Ethernet ports.

Data Planning

Configuration Item	Data
Port	Upstream port: 0/0/1 Service port: 0/3/1
SVLAN	VLAN ID: 300 VLAN type: smart VLAN attribute: common
Traffic profile	Profile ID: 8 Assured rate: no rate limit Priority source: user-cos Default priority: 4

Procedure

Step 1 Remotely log in to an ONU to configure the ONU.

You can remote log in to the ONU from the OLT to perform the configuration. User name: **root** (default); password: **mduadmin** (default)

Copyright © Huawei Technologies Co., Ltd.

Step 2 Create an SVLAN 300.

```
huawei(config)#vlan 300 smart
```

Step 3 Add upstream port 0/0/1 to the SVLAN.

```
huawei(config)#port vlan 300 0/0 1
```

Step 4 Configure a traffic profile.

Configure traffic profile 8. The upstream and downstream rates are not limited. Packets transmitted upstream use the priority (4 by default) copied from the user side. Packets transmitted downstream use the priority carried by themselves.

```
huawei(config)#traffic table ip index 8 cir off priority user-cos 4 priority-policy tag-in-package
```

Step 5 Add a service port.

Add a service port and bind it to port 0/3/1. Set the user VLAN to untagged and bind it to traffic profile 8.

```
huawei(config)#service-port vlan 300 eth 0/3/1 multi-service user-vlan untagged rx-cttr 8 tx-cttr 8
```

NOTE

Packets sent from the user side (IP PBX) may be transmitted upstream with a VLAN tag. In this case, change **untagged** to the VLAN tag when configuring a service port.

----End

13.3.3.7 Configuring Congestion Control and Security Policies

This topic describes how to configure global priority-based scheduling policies for queues to ensure service reliability and configure global security policies to ensure service security.

Context

Congestion control uses queue scheduling technology to map packets sent from the same port into multiple queues and process packets in each queue based on priority. Congestion control is recommended.

Security policies cover system security, user security, and service security, which ensure normal running of services.

NOTE

Enable security features based on service types. For details, see **13.2.5 Principle of Security Data Plan**.

Procedure

- Configure queue scheduling.

  Based on **13.2.3 Principle of QoS Data Plan**, all packets use strict priorities for queue scheduling and are mapped to queues based on priorities.

  ```
  huawei(config)#queue-scheduler strict-priority
  huawei(config)#cos-queue-map cos0 0 cos1 1 cos2 2 cos3 3 cos4 4 cos5 5 cos6 6 cos7 7  //System default
  ```

- Configure system security.
  - Enable deny of service (DoS) anti-attack on both the OLT and optical network units (ONUs).

Copyright © Huawei Technologies Co., Ltd.

1. Run the **security anti-dos enable** command to globally enable DoS anti-attack.
2. Run the **security anti-dos control-packet policy** command to configure a protocol packet processing policy that will be used when a DoS attack occurs.
3. Run the **security anti-dos control-packet rate** command to configure the threshold for the rate of sending protocol packets to the CPU.

- Enable IP address anti-attack on both the OLT and ONUs.

  Run the **security anti-ipattack enable** command to enable IP address anti-attack.

- Configure user security.
  - Enable MAC address anti-flapping on both the OLT and ONUs.

    Run the **security anti-macduplicate enable** command to enable MAC address anti-flapping.
  - Enable MAC address anti-spoofing on both the OLT and ONUs.
    1. In global config mode, run the **security anti-macspoofing enable** command to globally enable MAC address anti-spoofing.
    2. Enable MAC address anti-spoofing at VLAN level in global config mode or service profile mode:
       a. In global config mode, run the **security anti-macspoofing vlan** command to enable MAC address anti-spoofing.
       b. Perform the following operations to enable MAC address anti-spoofing in service profile mode:
          a. In global config mode, run the **vlan service-profile** command to create a VLAN service profile.
          b. Run the **security anti-macspoofing enable** command to enable MAC address anti-spoofing at VLAN level.
          c. Run the **commit** command to make the profile configuration take effect.
          d. Run the **quit** command to quit the VLAN service profile mode.
          e. Run the **vlan bind service-profile** command to bind the created VLAN service profile to a VLAN.
    3. (Optional) Run the **security anti-macspoofing max-mac-count** command to set the maximum number of MAC addresses that can be bound to a service flow.
    4. (Optional) Run the **security anti-macspoofing exclude** command to configure the types of packets for which MAC address anti-spoofing does not take effect, such as Internet Group Management Protocol (IGMP) packets.
  - Enable IP address anti-spoofing on ONUs.

    IP address anti-spoofing can be enabled or disabled at three levels: global, VLAN, and service port levels. This function takes effect only after it is enabled at the three levels. Among the three levels, IP address anti-spoofing is disabled only at the global level by default.
    1. In global config mode, run the **security anti-ipspoofing enable** command to enable IP address anti-spoofing at the global level.
    2. In VLAN service profile mode, run the **security anti-ipspoofing enable** command to enable IP address anti-spoofing at the VLAN level.

Copyright © Huawei Technologies Co., Ltd.

3. Run the **security anti-ipspoofing service-port** *serviceport-id* **enable** command to enable IP address anti-spoofing at the service port level.

----End

13.3.3.8 Configuring E2E Reliability

This topic describes how to configure end-to-end (E2E) protection schemes for the enterprise private line service which has a high requirement on service reliability.

Context

Reliability covers equipment reliability, upstream networking protection, and downstream networking protection. For details on reliability data planning, see **13.2.6 Principle of Reliability Data Plan**.

- Upstream networking protection includes link aggregation group and protection group. Usually, link aggregation group is configured when the GIU board is used to transmit traffic upstream; protection group is configured when the main control board is used to transmit traffic upstream. The two protection schemes are not configured at the same time.
- Downstream networking protection includes Type B, Type C single homing, and Type C dual homing, which are used to protect service ports. Ports on the same ONU can be configured only with the same protection scheme.

NOTE

This topic describes how to configure five mainstream protection schemes. Select required protection schemes based on the carrier's requirement and actual networking scenario.

Procedure

- Configure a link aggregation group.

  Bind upstream ports 0/19/0 and 0/19/1 together as an aggregation link group. Each member port in the group transmits packets based on source MAC addresses. The working mode is LACP static aggregation.

  ```
  huawei(config)#link-aggregation 0/19 0-1 ingress workmode lacp-static
  ```

- Configure a protection group.

  Configure upstream ports 0/19/0 and 0/19/1 on board GIU as a port protection group. Set port 0/19/0 as the working port and port 0/19/1 as the protection port, set the working mode to time delay detection, and enable the protection group.

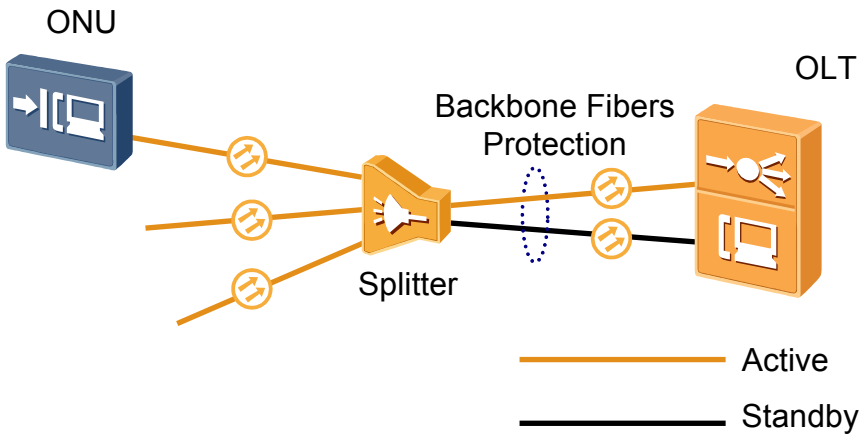
  ```
  huawei(config-protect)#protect-group first 0/19/0 second 0/19/1 eth workmode timedelay enable
  ```

- Configure the Type B protection.

  Figure 13-9 shows the Type B protection networking diagram.

Copyright © Huawei Technologies Co., Ltd.

Figure 13-9 Type B protection



Configure redundancy backup for ports 0/3/1 and 0/3/2 on the same GPON board on OLT. When port 0/3/1 fails, the system can automatically switch to port 0/3/2.

```
huawei(config)#protect-group 0 protect-target gpon-uni-port workmode timedelay
huawei(protect-group-0)#protect-group member port 0/3/1 role work
huawei(protect-group-0)#protect-group member port 0/3/2 role protect
huawei(protect-group-0)#protect-group enable
```

NOTE

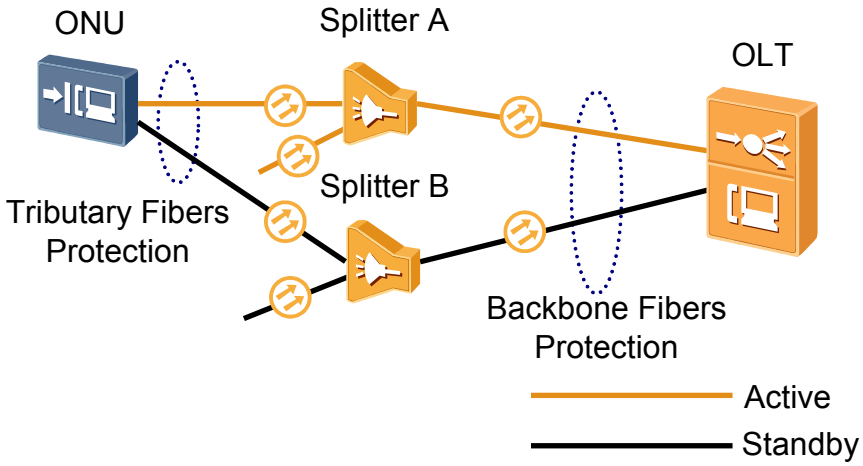
The configurations of services accessed by the ONUs remain the same after the Type B protection is configured. That is, the service configurations are applied only to the working GPON port.

- Configure the Type C single homing protection.

  Figure 13-10 shows networking diagram for the Type C single homing protection. Configure two 1:N optical splitters, one for connecting the working PON ports on the OLT and ONUs, and one for connecting the protection PON ports on the OLT and ONUs. This protection scheme protects both the backbone fibers and tributary fibers.

  The configurations of services accessed by the ONUs remain the same after the Type C single homing protection is configured. That is, the service configurations are applied only to the working PON port on the OLT and working upstream PON ports on the ONUs.

Figure 13-10 Type C single homing protection



Copyright © Huawei Technologies Co., Ltd.

As shown in the preceding figure, Type C single homing protecting is configured for optical fiber links between the OLT and ONU.

- The ports on the GPON service board are 0/3/1 and 0/3/2.
- The link at port 0/3/1 is the working link.
- The link at port 0/3/2 is the protection link.
- The ONU ID is 1.
- The ONU is authenticated by serial number (SN). The SN of the ONU is 32303131B39FD641 and the management mode is SNMP.
- The ID of the line profile bound to the ONU is 10.

```
huawei(config)#interface gpon 0/3
huawei(config-if-gpon-0/3)#ont add 1 1 sn-auth 32303131B39FD641 snmp ont-
lineprofile-id 10
huawei(config-if-gpon-0/3)#ont add 2 1 protect-side
huawei(config-if-gpon-0/3)#quit
huawei(config)#protect-group protect-target gpon-uni-ont workmode portstate
huawei(protect-group-1)#protect-group member port 0/3/1 ont 1 role work
huawei(protect-group-1)#protect-group member port 0/3/2 ont 1 role protect
huawei(protect-group-1)#protect-group enable
huawei(protect-group-1)#quit
```

- Configure the Type C dual homing protection.

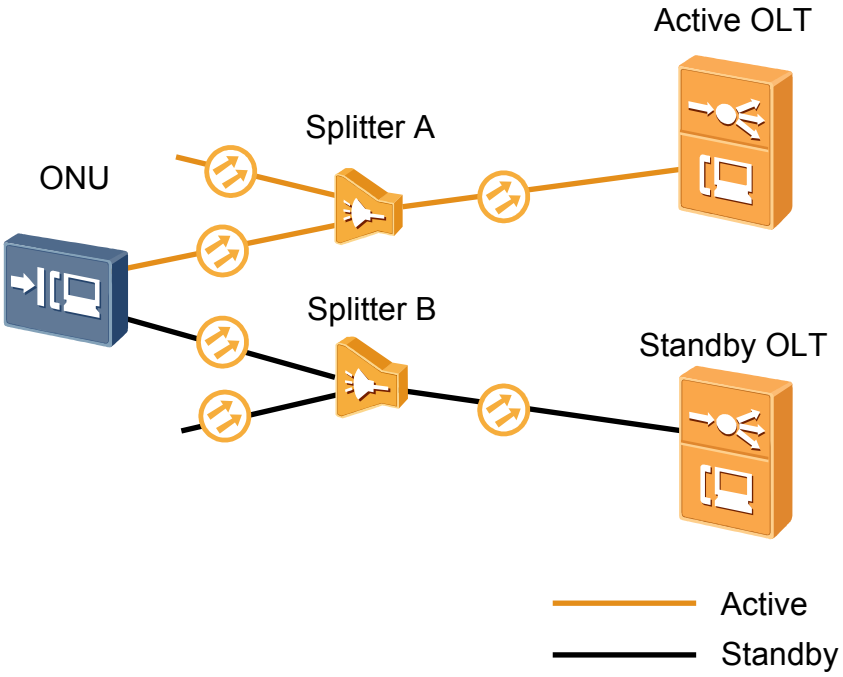
  Figure 13-11 shows the networking diagram for the Type C dual homing protection. Two PON ports on different OLTs, two PON ports on an ONU, two backbone optical fibers, two optical splitters, and two tributary optical fibers are configured to implement this protection. The difference between this protection scheme and the Type C single homing protection scheme is that the ONU needs to be dual homed to two OLTs in this protection scheme.

  The models and versions of main control boards on the active and standby OLTs must be the same. The models and versions of GPON boards on the active and standby OLTs also must be the same. Data on the active OLT cannot be automatically synchronized with that on the standby OLT. Therefore, data synchronization between the active and standby OLTs must be manually ensured.

  This protection scheme can be configured for only the Ethernet QinQ private line service. It does not support TDM services, including Native TDM and SAToP.

Copyright © Huawei Technologies Co., Ltd.

Figure 13-11 Type C dual homing protection



As shown in the preceding figure, Type C dual homing protection is configured for two OLTs (huawei_A and huawei_B).

- huawei_A is the active OLT while huawei_B is the standby OLT.
- The ports on the service boards on both OTLs are 0/3/1.
- The dual homing protection group ID is 1.
- The ONU ID is 1.
- The ONU is authenticated by serial number (SN). The SN of the ONU is 32303131B39FD641 and the management mode is SNMP.
- The ID of the line profile bound to the ONU is 10.

```
Configurations on the active OLT huawei_A:
huawei_A(config)#interface gpon 0/3
huawei_A(config-if-gpon-0/3)#ont add 1 1 sn-auth 32303131B39FD641 snmp ont-
lineprofile-id 10
huawei_A(config-if-gpon-0/3)#quit
huawei_A(config)#protect-group 1 protect-target gpon-uni-ont workmode dual-
parenting
huawei_A(protect-group-1)#protect-group member port 0/3/1 ont 1 role work
Configurations on the standby OLT huawei_B:
huawei_B(config)#interface gpon 0/3
huawei_B(config-if-gpon-0/3)#ont add 1 1 sn-auth 32303131B39FD641 snmp ont-
lineprofile-id 10
huawei_B(config-if-gpon-0/3)#quit
huawei_B(config)#protect-group 1 protect-target gpon-uni-ont workmode dual-
parenting
huawei_B(protect-group-1)#protect-group member port 0/3/1 ont 1 role protect
huawei_B(protect-group-1)#protect-group enable
```

----End

Copyright © Huawei Technologies Co., Ltd.

13.3.3.9 Verifying Services

This topic describes how to verify the IP PBX access service by testing calls.

Prerequisites

The IP PBX access service has been deployed.

Procedure

Step 1 Test calls between users connected to the IP PBX according to table 1.

Step 2 Test calls from a user connected to the IP PBX to an IMS user according to table 1.

Step 3 Test calls from an IMS user to a user connected to the IP PBX according to table 1.

Table 13-6 IP PBX access service verification

Category	Test Calls Between Users Connected to the IP PBX	Test Calls from a User Connected to the IP PBX to an IMS User	Test Calls from an IMS User to a User Connected to the IP PBX
Prerequisites	1. User A and user B access the network through the IP PBX and both users have been registered. 2. User A and user B are idle.	1. User A accesses the network through the IP PBX and has been registered. 2. User B is a common IMS user and has been registered. 3. User A and user B are idle.	1. User A is a common IMS user and has been registered. 2. User B accesses the network through the IP PBX and has been registered. 3. User A and user B are idle.
Test procedure	1. User A calls user B. 2. User B answers the call. Check the call between user A and user B. 3. User A releases the call.	The same as that in the "Test Calls Between Users Connected to the IP PBX" column	The same as that in the "Test Calls Between Users Connected to the IP PBX" column
Expected result	1. User B hears the ringing tone. 2. The call is set up. 3. The call is released.	The same as that in the "Test Calls Between Users Connected to the IP PBX" column	The same as that in the "Test Calls Between Users Connected to the IP PBX" column

----End

Copyright © Huawei Technologies Co., Ltd.

13.3.4 Enterprise PRA PBX Private Line Access Service

ONUs provide PRA E1 ports to access PRA private branch exchange (PBX) services of an enterprise and transmit them to an OLT. Then, the OLT forwards the service data upstream to the packet switched network (PSN). This achieves voice-to-IP conversion, simplifying the network architecture.

13.3.4.1 Service Requirement and Application Scenario

Service Requirement

PRA PBX is a telephone exchange used in an enterprise. With the PRA PBX, staff in the enterprise can use internal telephones to make free calls by dialing short numbers. Outgoing calls are made through a unified trunk. After the PRA PBX service is accessed in PON mode using "OLT+ONU", VoIP calls can be made. Compared with services provided by the PRA PBX itself, the VoIP service has following advantages:

- Outgoing call data is carried over IP, which greatly lowers communication costs for enterprises and retains good call quality.
- No extra investment is required because the voice service is deployed directly using the PRA PBX.
- Free calls can be made between branches in different regions.
- More value-added services can be provided based on IP networks.

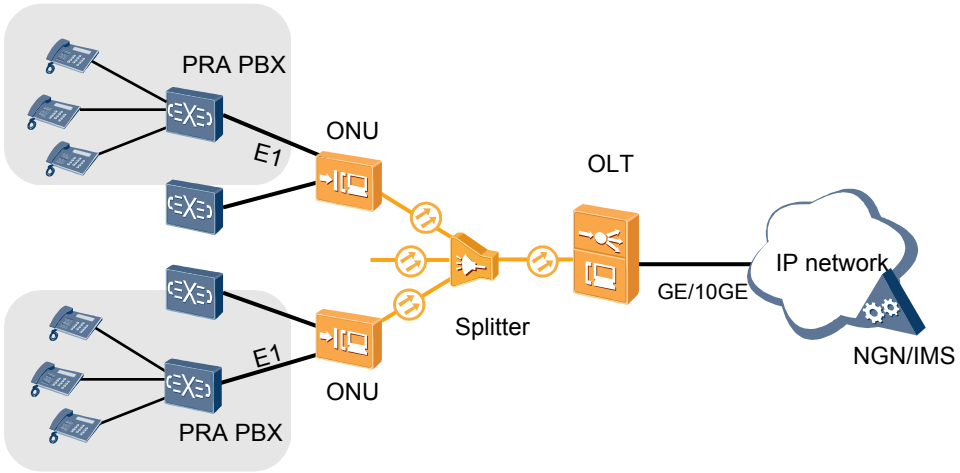
In addition, the operation method for end users connected to the PRA PBX is not changed.

Application Scenario

As shown in **Figure 13-12**, ONUs access PRA PBX services through E1 lines. The OLT transmits the data to the upper NGN/IMS, achieving the VoIP-based PRA voice service.

Applicable ONU: MA5612, MA5616.

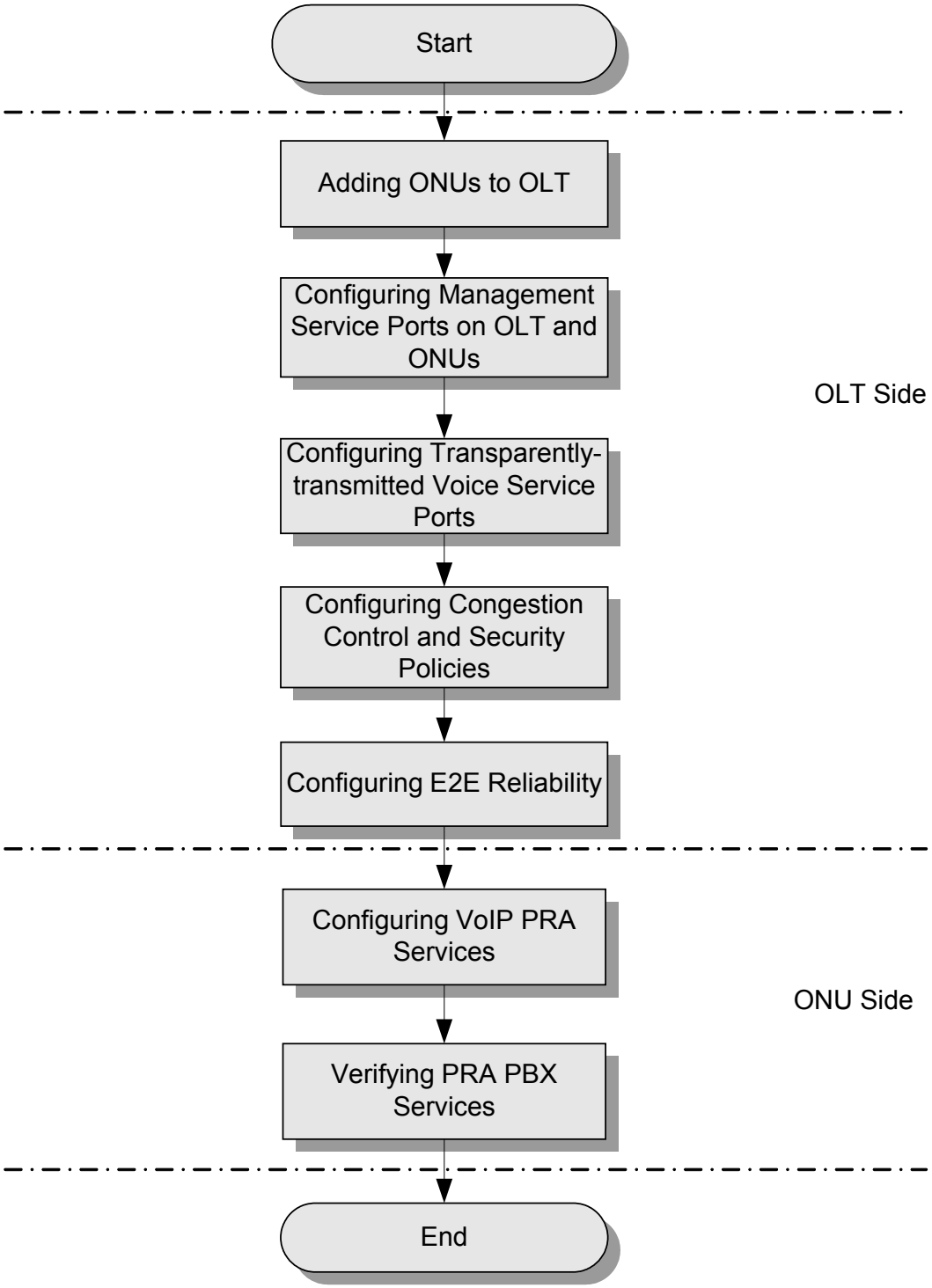
Figure 13-12 Networking diagram of the PRA PBX access service



Copyright © Huawei Technologies Co., Ltd.

13.3.4.2 Configuration Process

The following figure shows the configuration process for the PRA PBX access service.



13.3.4.3 Adding ONUs to OLT

This topic describes how to add ONUs to the OLT. ONUs can be configured only after they are added to the OLT successfully.

Copyright © Huawei Technologies Co., Ltd.

Context

- When adding ONUs, you need to bind related profiles to the ONUs, including the DBA profile, line profile, and alarm profile.
- An ONU can be added in two modes: offline addition and online confirmation. Select either mode as required.

Data Planning

Table 13-7 Key data plan

Configuration Item	Data
DBA profile	Profile ID: 20 Profile type: Type 3 Assured bandwidth: 100 Mbit/s Maximum bandwidth: 120 Mbit/s
Line profile	Profile ID: 10 T-CONT ID: 4 GEM port ID for management service: 11 GEM port ID for other services: 12
Networking data	PON port: 0/3/1 ONU parameters: ● ONU ID: 1 ● SN: 32303131B39FD641

Procedure

Step 1 Configure GPON ONU profiles.

1. Configure a DBA profile.

```
huawei(config)#dba-profile add profile-id 20 type3 assure 102400 max 122880
```

2. Configure an ONU line profile.

```
huawei(config)#ont-lineprofile gpon profile-id 10
huawei(config-gpon-lineprofile-10)#tcont 4 dba-profile-id 20  //Bind T-CONT 4 to DBA profile 20
huawei(config-gpon-lineprofile-10)#gem add 11 eth tcont 0
huawei(config-gpon-lineprofile-10)#gem add 12 eth tcont 4 //Add GEM port 12 to T-CONT 4
huawei(config-gpon-lineprofile-10)#gem mapping 11 0 vlan 8
huawei(config-gpon-lineprofile-10)#gem mapping 12 1 vlan 300 //Map GEM port 12 to CVLAN 300
huawei(config-gpon-lineprofile-10)#commit
huawei(config-gpon-lineprofile-10)#quit
```

3. (Optional) Configure an alarm profile.

Copyright © Huawei Technologies Co., Ltd.

- The default GPON alarm profile ID is 1. The value of each alarm threshold is **0** which indicates that alarms are not reported.
- In this example, the default alarm profile is used and no configuration is required.

Step 2 Add ONUs to the OLT.

1. Add ONU 1 in offline mode.

```
huawei(config)#interface gpon 0/3
huawei(config-if-gpon-0/3)#ont add 1 ontid 1 sn-auth 32303131B39FD641
snmp ont-lineprofile-id 10
```

2. (Optional) Bind an alarm profile.

   By default, an ONU will be automatically bound to alarm profile 1 (default profile). You need to manually bind an alarm profile to an ONU only when the default alarm profile does not meet requirements.

   In this example, the default alarm profile is used. Therefore, you do not need to manually bind an alarm profile.

Step 3 Confirm the ONU status.

After adding an ONU, run the **display ont info** command to query the current status of the ONU. Ensure that **Control flag** is **active**, **Run State** is **online**, and **Config state** is **normal**.

The following uses ONU 1 as an example to describe how to confirm ONU status.

```
huawei(config-if-gpon-0/3)#display ont info 1 1
  ------------------------------------------------------------------------
  F/S/P                : 0/3/1
  ONT-ID               : 1
  Control flag         : active    //Indicates that the ONU is
activated.
  Run state            : online    //Indicates that the ONU is
online.
  Config state         : normal    //Indicates that the ONU is in normal
state.
...//Other command output is omitted.
huawei(config-if-gpon-0/3)#quit
```

----End

Follow-up Procedure

When **Config state** is **failed**, **Run state** is **offline**, or **Match state** is **mismatch**:

- If **Control flag** is **deactive**, run the **ont active** command in GPON mode to activate the ONU.
- If **Run state** is **offline**, a physical line may be broken or the optical module may be damaged. Check the line and the optical module.
- If **Config state** is **failed**, the configured ONU capability exceeds the actual ONU capability. In this case, run the **display ont failed-configuration** command in the diagnose mode to check the failed configuration item and the failure cause. Then, rectify the fault accordingly.
- If the ONU does not match, that is, **Match state** is **mismatch**, the port types and number of ports undermatch the actual port types and number of ports supported by the ONU. In this case, run the **display ont capability** command to query the actual capability of the ONU, and then select one of the following modes to modify the ONU configuration:
  - Create a proper ONU profile according to the actual capability of the ONU, and then run the **ont modify** command to modify the configuration data of the ONU.

Copyright © Huawei Technologies Co., Ltd.

- Modify the ONU profile according to the actual capability of the ONU and save the modification. Then, the ONU automatically recovers the configuration successfully.

13.3.4.4 Configuring Management Service Ports on OLT and ONUs

This topic describes how to configure management service ports (also called service flows) on the OLT and ONUs. After the connections between the in-band management service ports on the OLT and ONUs are reachable, you can log in to the ONUs on the OLT and configure the ONUs.

Data Plan

Configuration Item	Data
Management VLAN and management IP address for OLT	Management VLAN ID: 8 Management VLAN type: smart In-band management IP address: 192.168.50.1/24
Management VLAN and management IP address for ONU	Management VLAN ID: 8 Management VLAN type: smart In-band management IP address for ONU 3: 192.168.50.2/24

Procedure

Step 1 Configure the in-band management VLAN and IP address for the OLT.

Set the in-band management VLAN to 8, VLAN priority to 6, and IP address to 192.168.50.1/24.

```
huawei(config)#vlan 8 smart
huawei(config)#port vlan 8 0/19 0
huawei(config)#vlan priority 8 6
huawei(config)#interface vlanif 8
huawei(config-if-vlanif8)#ip address 192.168.50.1 24
huawei(config-if-vlanif8)#quit
```

Step 2 Configure the in-band management VLAN and IP address for the ONU.

```
huawei(config)#interface gpon 0/3
huawei(config-if-gpon-0/3)#ont ipconfig 1 1 static ip-address 192.168.50.2 mask
255.255.255.0 gateway
192.168.50.1 vlan 8
huawei(config-if-gpon-0/3)#quit
```

Step 3 Configure the in-band management service port.

Set the management VLAN to 8, GEM port ID to 11, and user VLAN to 8. The OLT does not rate limit the in-band management service port. Therefore, directly use the default traffic profile 6.

```
huawei(config)#service-port vlan 8 gpon 0/3/1 ont 1 gemport 11 multi-service
user-vlan 8 rx-cttr 6 tx-cttr 6
```

Step 4 Confirm that the connection between the management service ports on the OLT and ONU is reachable.

Copyright © Huawei Technologies Co., Ltd.

- Run the **ping *ONU ip*** command on the OLT to verify the connectivity between the OLT and ONU. If the OLT receives ICMP ECHO-REPLY packets from the ONU, the connection is reachable.
- When the connection is reachable, you can remote log in to the ONU from the OLT and configure the ONU.

----End

13.3.4.5 Configuring Service Ports for Voice Transparent Transmission

This topic describes how to create service ports on the OLT to transparently transmit VoIP service data from ONUs to the upper-layer voice server.

Data Plan

Configuration Item	Data
SVLAN	VLAN ID: 300 VLAN attribute: common
CVLAN (upstream VALN of the ONU)	300
Traffic profile	Profile ID: 10 Assured bandwidth: 100 Mbit/s Priority source: user-cos Default priority: 5

NOTE

The VoIP service is a self-operated service. The single SVLAN is a mainstream application and is recommended.

Procedure

Step 1 Configure an SVLAN and add an upstream port to it.

Set the SVLAN ID of the PRA PBX service to 300, VLAN type to smart, and add upstream port 0/19/0 to the VLAN.

```
huawei(config)#vlan 300 smart
huawei(config)#port vlan 300 0/19 0
```

Step 2 Configure a traffic profile for the service port.

Add a new traffic profile 10 and set the assured rate to 100 Mbit/s. Packets transmitted upstream use the priority (5 by default) copied from the user side. Packets transmitted downstream use the priority carried by themselves.

```
huawei(config)#traffic table ip index 10 cir 102400 priority user-cos 5 priority-policy tag-in-package
```

Step 3 Configure a service port.

Copyright © Huawei Technologies Co., Ltd.

According to **13.2.2 Principle of VLAN Data Plan**, VLANs of packets sent from the PRA PBX are all translated to CLVAN 300. The OLT transparently transmits the packets. The traffic profile 10 is used.

```
huawei(config)#service-port vlan 300 gpon 0/3/1 ont 1 gemport 12 multi-service
user-vlan 300 rx-cttr 10 tx-cttr 10
```

----End

13.3.4.6 Configuring VoIP PRA Access

This topic describes how to configure VoIP PRA access. ONUs provide PRA E1 ports to access the PRA PBX service and convert PRA signaling to ISDN Q.931-User Adaptation Layer (IUA) signaling, achieving signaling exchange between ONUs and media gateway controller (MGCs).

Prerequisites

The H.248 protocol is a master/slave protocol which is used by an MGC to control access gateways (AGs) to implement call connections. The data, including media gateway (MG) interface attributes and voice user attributes on AGs, must be consistent with those on the MGC. Therefore, before configuring the VoIP voice service, plan data with the MGC.

Context

IUA is the ISDN Q.931-User Adaptation Layer protocol. IUA links carry signaling exchanged between ONUs and MGCs.

Data Plan

Table 13-8 Data plan for VoIP PRA service

Configuration Item	Data
VLAN	VLAN ID: 300 IP address of the Layer 3 interface: 10.10.10.10/24
MG interface	MG ID: 0 Media/signaling IP address: 10.10.10.10/24 MGC IP address: 200.200.200.200 Gateway IP address: 10.10.10.1 Protocol port: 2944
IUA linkset	IUA link set ID: 1 Working mode of the link set: override Interface ID (IID) generation mode: 2 Service environment of the IUA link set: client Interlocking function: enabled

Copyright © Huawei Technologies Co., Ltd.

Configuration Item	Data
IUA link	IUA link ID: 0 Local port ID: 1402 Local IP address: 10.10.10.10 Remote port ID: 1404 Remote IP address for the primary MGC: 200.200.200.200 Interlocking policy: the link switches over with the primary MAC
PRA port	Subrack ID/slot ID/port ID: Terminal ID: 512

Procedure

Step 1 Configure an upstream VLAN and VLAN interface.

Specify an upstream VLAN interface for the media stream and signaling flow, and set the IP addresses of the Layer 3 interface. These IP addresses are the sources of the media and signaling IP address pools.

1. Create an upstream VLAN 300 and add upstream port 0/0/1 to the VLAN.

```
huawei(config)#vlan 300 smart
huawei(config)#port vlan 300 0/0 1
```

2. Configure the IP address of Layer 3 interface.

   Enter the VLAN interface mode and set the IP address of the Layer 3 interface to 10.10.10.10.

```
huawei(config)#interface vlanif 300
huawei(config-if-vlanif300)#ip address 10.10.10.10 24
huawei(config-if-vlanif300)#quit
```

Step 2 Configure the media and signaling IP address pools.

The media and signaling IP addresses are 10.10.10.10, and the media gateway IP address is 10.10.10.1.

```
huawei(config)#voip
huawei(config-voip)#ip address media 10.10.10.10 10.10.10.1
huawei(config-voip)#ip address signaling 10.10.10.10
huawei(config-voip)#quit
```

NOTE

The media IP address can be different from the signaling IP address. You can make data plan according to the actual network situation.

Step 3 Configure a static route.

Because the IP address of the VLAN interface and the IP address of the MGC (200.200.200.200/24) are in different network segments, a route from gateway 10.10.10.1 to 200.200.200.0 network segment must be configured.

```
huawei(config)#ip route-static 200.200.200.0 24 10.10.10.1
```

Step 4 Add an MG interface and configure interface attributes.

Copyright © Huawei Technologies Co., Ltd.

1. Add an MG interface.

   Add an MG interface for the MG to communicate with the MGC, which ensures that the MGC can control call connections through the MG interface. Add MG interface 0 according to the data plan.

```
huawei(config)#interface h248 0
  Are you sure to add MG interface?(y/n)[n]:y
```

2. Configure MG interface attributes.

   Configure MG interface attributes according to the data plan. When configuring the attributes, note that:

   - The registration mode of the MG interface must be consistent with that on the MGC. Registration mode: by IP address (default) or by domain name
   - H.248 version for negotiation: H.248v1, H.248v2, or H.248v3 (default). When H.248v3 is used, interfaces fail to be registered if some softswitches do not support H.248v3.

```
huawei(config-if-h248-0)#if-h248 attribute mgip 10.10.10.10 mgport
 2944 code text transfer udp primary-mgc-ip1 200.200.200.200 primary-mgc-port
 2944 mg-media-ip1 10.10.10.10 start-negotiate-version 1
```

3. Enable the MG interface.

```
huawei(config-if-h248-0)#reset coldstart
  Are you sure to reset MG interface?(y/n)[n]:y
huawei(config-if-h248-0)#quit
```

   NOTE

   - After configuring the MG interface, you must perform a cold reset on the interface. Otherwise, the interface cannot take effect.
   - You can perform a cold reset on the MG interface only after the following parameters are correctly configured: **mgip**, **mgport**, **primary-mgc-ip1** (or **mgc-domain-name1**), **mgcport_1**, **code**, **transfer**, and **mg-media-ip**.

4. Query the running status of the MG interface.

   If the MG interface is interconnected with the MGC successfully, the MG interface is in normal state which indicates that the interface is working properly.

```
huawei(config)#display if-h248 all
  ------------------------------------------------------------------------
  MGID   Trans     State    MGPort MGIP           MGCPort MGCIP/DomainName
  ------------------------------------------------------------------------
  0      UDP       Normal   2944   10.10.10.10     2944    200.200.200.200
  ------------------------------------------------------------------------
```

Step 5 Configure IUA links.

In the sigtran mode, configure the Signaling Transport protocol stack. Add an IUA link set first and then add IUA links.

```
huawei(config)#sigtran
huawei(config-sigtran)#iua-linkset add 1 mgid 0 jointly-work enable trafficmode
override iid-map 2 cs-mode client
huawei(config-sigtran)#iua-link add 0 1 1402 10.10.10.10 1404 200.200.200.200
jointly-work-with primary-mgc
huawei(config-sigtran)#quit
```

Step 6 Add ISDN PRA user.

```
huawei(config)#esl user
huawei(config-esl-user)#mgprauser add  0 1 interfaceid 0 terminalid 512
```

----End

Copyright © Huawei Technologies Co., Ltd.

13.3.4.7 Configuring Congestion Control and Security Policies

This topic describes how to configure global priority-based scheduling policies for queues to ensure service reliability and configure global security policies to ensure service security.

Context

Congestion control uses queue scheduling technology to map packets sent from the same port into multiple queues and process packets in each queue based on priority. Congestion control is recommended.

Security policies cover system security, user security, and service security, which ensure normal running of services.

NOTE

Enable security features based on service types. For details, see **13.2.5 Principle of Security Data Plan**.

Procedure

- Configure queue scheduling.

  Based on **13.2.3 Principle of QoS Data Plan**, all packets use strict priorities for queue scheduling and are mapped to queues based on priorities.

  ```
  huawei(config)#queue-scheduler strict-priority
  huawei(config)#cos-queue-map cos0 0 cos1 1 cos2 2 cos3 3 cos4 4 cos5 5 cos6 6 cos7 7  //System default
  ```

- Configure system security.
  - Enable deny of service (DoS) anti-attack on both the OLT and optical network units (ONUs).
    1. Run the **security anti-dos enable** command to globally enable DoS anti-attack.
    2. Run the **security anti-dos control-packet policy** command to configure a protocol packet processing policy that will be used when a DoS attack occurs.
    3. Run the **security anti-dos control-packet rate** command to configure the threshold for the rate of sending protocol packets to the CPU.
  - Enable IP address anti-attack on both the OLT and ONUs.

    Run the **security anti-ipattack enable** command to enable IP address anti-attack.
- Configure user security.
  - Enable MAC address anti-flapping on both the OLT and ONUs.

    Run the **security anti-macduplicate enable** command to enable MAC address anti-flapping.
  - Enable MAC address anti-spoofing on both the OLT and ONUs.
    1. In global config mode, run the **security anti-macspoofing enable** command to globally enable MAC address anti-spoofing.
    2. Enable MAC address anti-spoofing at VLAN level in global config mode or service profile mode:
       a. In global config mode, run the **security anti-macspoofing vlan** command to enable MAC address anti-spoofing.
       b. Perform the following operations to enable MAC address anti-spoofing in service profile mode:

Copyright © Huawei Technologies Co., Ltd.

a. In global config mode, run the **vlan service-profile** command to create a VLAN service profile.
b. Run the **security anti-macspoofing enable** command to enable MAC address anti-spoofing at VLAN level.
c. Run the **commit** command to make the profile configuration take effect.
d. Run the **quit** command to quit the VLAN service profile mode.
e. Run the **vlan bind service-profile** command to bind the created VLAN service profile to a VLAN.

3. (Optional) Run the **security anti-macspoofing max-mac-count** command to set the maximum number of MAC addresses that can be bound to a service flow.
4. (Optional) Run the **security anti-macspoofing exclude** command to configure the types of packets for which MAC address anti-spoofing does not take effect, such as Internet Group Management Protocol (IGMP) packets.

- Enable IP address anti-spoofing on ONUs.

  IP address anti-spoofing can be enabled or disabled at three levels: global, VLAN, and service port levels. This function takes effect only after it is enabled at the three levels. Among the three levels, IP address anti-spoofing is disabled only at the global level by default.

  1. In global config mode, run the **security anti-ipspoofing enable** command to enable IP address anti-spoofing at the global level.
  2. In VLAN service profile mode, run the **security anti-ipspoofing enable** command to enable IP address anti-spoofing at the VLAN level.
  3. Run the **security anti-ipspoofing service-port** *serviceport-id* **enable** command to enable IP address anti-spoofing at the service port level.

----End

13.3.4.8 Configuring E2E Reliability

This topic describes how to configure end-to-end (E2E) protection schemes for the enterprise private line service which has a high requirement on service reliability.

Context

Reliability covers equipment reliability, upstream networking protection, and downstream networking protection. For details on reliability data planning, see **13.2.6 Principle of Reliability Data Plan**.

- Upstream networking protection includes link aggregation group and protection group. Usually, link aggregation group is configured when the GIU board is used to transmit traffic upstream; protection group is configured when the main control board is used to transmit traffic upstream. The two protection schemes are not configured at the same time.
- Downstream networking protection includes Type B, Type C single homing, and Type C dual homing, which are used to protect service ports. Ports on the same ONU can be configured only with the same protection scheme.

NOTE

This topic describes how to configure five mainstream protection schemes. Select required protection schemes based on the carrier's requirement and actual networking scenario.

Copyright © Huawei Technologies Co., Ltd.

Procedure

- Configure a link aggregation group.

  Bind upstream ports 0/19/0 and 0/19/1 together as an aggregation link group. Each member port in the group transmits packets based on source MAC addresses. The working mode is LACP static aggregation.

  ```
  huawei(config)#link-aggregation 0/19 0-1 ingress workmode lacp-static
  ```

- Configure a protection group.

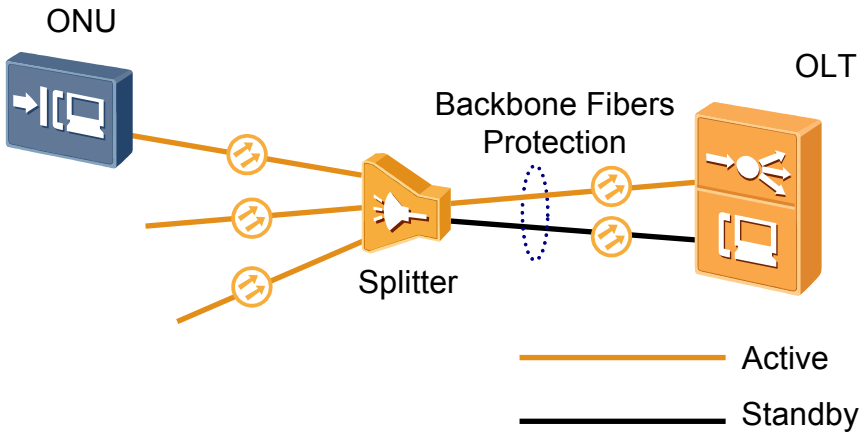
  Configure upstream ports 0/19/0 and 0/19/1 on board GIU as a port protection group. Set port 0/19/0 as the working port and port 0/19/1 as the protection port, set the working mode to time delay detection, and enable the protection group.

  ```
  huawei(config-protect)#protect-group first 0/19/0 second 0/19/1 eth workmode timedelay enable
  ```

- Configure the Type B protection.

  Figure 13-13 shows the Type B protection networking diagram.

  Figure 13-13 Type B protection

  Configure redundancy backup for ports 0/3/1 and 0/3/2 on the same GPON board on OLT. When port 0/3/1 fails, the system can automatically switch to port 0/3/2.

  ```
  huawei(config)#protect-group 0 protect-target gpon-uni-port workmode timedelay
  huawei(protect-group-0)#protect-group member port 0/3/1 role work
  huawei(protect-group-0)#protect-group member port 0/3/2 role protect
  huawei(protect-group-0)#protect-group enable
  ```

  NOTE

  The configurations of services accessed by the ONUs remain the same after the Type B protection is configured. That is, the service configurations are applied only to the working GPON port.

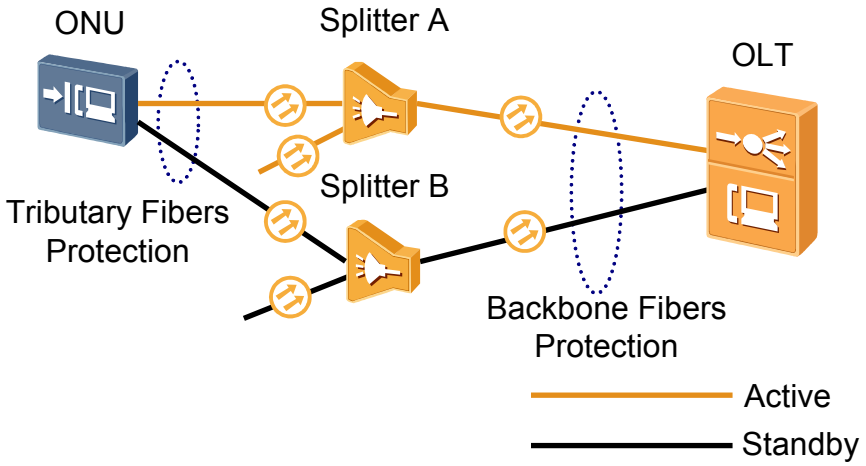
- Configure the Type C single homing protection.

  Figure 13-14 shows networking diagram for the Type C single homing protection. Configure two 1:N optical splitters, one for connecting the working PON ports on the OLT and ONUs, and one for connecting the protection PON ports on the OLT and ONUs. This protection scheme protects both the backbone fibers and tributary fibers.

  The configurations of services accessed by the ONUs remain the same after the Type C single homing protection is configured. That is, the service configurations are applied only to the working PON port on the OLT and working upstream PON ports on the ONUs.

Copyright © Huawei Technologies Co., Ltd.

Figure 13-14 Type C single homing protection



As shown in the preceding figure, Type C single homing protecting is configured for optical fiber links between the OLT and ONU.

- The ports on the GPON service board are 0/3/1 and 0/3/2.
- The link at port 0/3/1 is the working link.
- The link at port 0/3/2 is the protection link.
- The ONU ID is 1.
- The ONU is authenticated by serial number (SN). The SN of the ONU is 32303131B39FD641 and the management mode is SNMP.
- The ID of the line profile bound to the ONU is 10.

```
huawei(config)#interface gpon 0/3
huawei(config-if-gpon-0/3)#ont add 1 1 sn-auth 32303131B39FD641 snmp ont-lineprofile-id 10
huawei(config-if-gpon-0/3)#ont add 2 1 protect-side
huawei(config-if-gpon-0/3)#quit
huawei(config)#protect-group protect-target gpon-uni-ont workmode portstate
huawei(protect-group-1)#protect-group member port 0/3/1 ont 1 role work
huawei(protect-group-1)#protect-group member port 0/3/2 ont 1 role protect
huawei(protect-group-1)#protect-group enable
huawei(protect-group-1)#quit
```

- Configure the Type C dual homing protection.

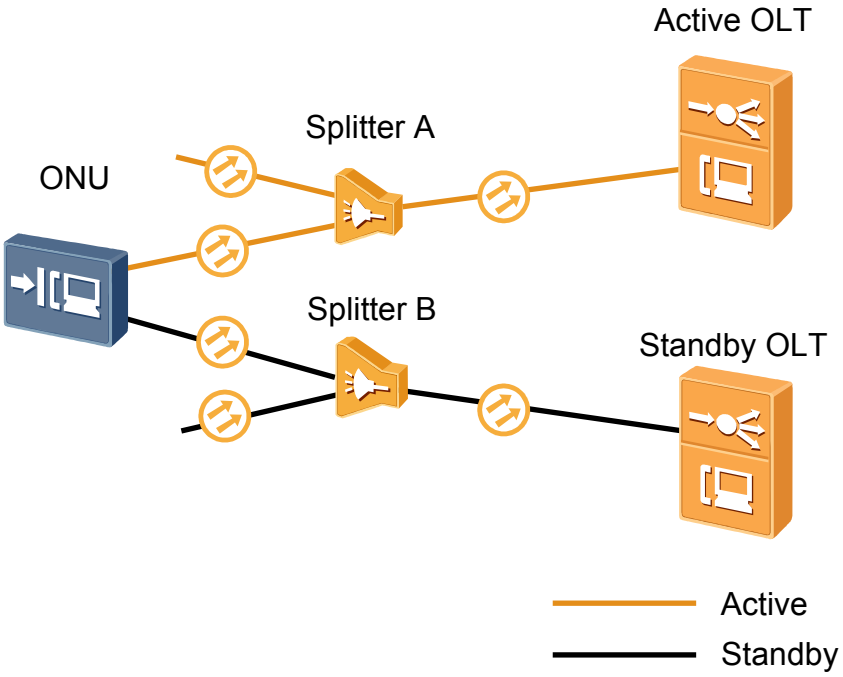
  Figure 13-15 shows the networking diagram for the Type C dual homing protection. Two PON ports on different OLTs, two PON ports on an ONU, two backbone optical fibers, two optical splitters, and two tributary optical fibers are configured to implement this protection. The difference between this protection scheme and the Type C single homing protection scheme is that the ONU needs to be dual homed to two OLTs in this protection scheme.

  The models and versions of main control boards on the active and standby OLTs must be the same. The models and versions of GPON boards on the active and standby OLTs also must be the same. Data on the active OLT cannot be automatically synchronized with that on the standby OLT. Therefore, data synchronization between the active and standby OLTs must be manually ensured.

  This protection scheme can be configured for only the Ethernet QinQ private line service. It does not support TDM services, including Native TDM and SAToP.

Copyright © Huawei Technologies Co., Ltd.

Figure 13-15 Type C dual homing protection



As shown in the preceding figure, Type C dual homing protection is configured for two OLTs (huawei_A and huawei_B).

- huawei_A is the active OLT while huawei_B is the standby OLT.
- The ports on the service boards on both OTLs are 0/3/1.
- The dual homing protection group ID is 1.
- The ONU ID is 1.
- The ONU is authenticated by serial number (SN). The SN of the ONU is 32303131B39FD641 and the management mode is SNMP.
- The ID of the line profile bound to the ONU is 10.

```
Configurations on the active OLT huawei_A:
huawei_A(config)#interface gpon 0/3
huawei_A(config-if-gpon-0/3)#ont add 1 1 sn-auth 32303131B39FD641 snmp ont-
lineprofile-id 10
huawei_A(config-if-gpon-0/3)#quit
huawei_A(config)#protect-group 1 protect-target gpon-uni-ont workmode dual-
parenting
huawei_A(protect-group-1)#protect-group member port 0/3/1 ont 1 role work
Configurations on the standby OLT huawei_B:
huawei_B(config)#interface gpon 0/3
huawei_B(config-if-gpon-0/3)#ont add 1 1 sn-auth 32303131B39FD641 snmp ont-
lineprofile-id 10
huawei_B(config-if-gpon-0/3)#quit
huawei_B(config)#protect-group 1 protect-target gpon-uni-ont workmode dual-
parenting
huawei_B(protect-group-1)#protect-group member port 0/3/1 ont 1 role protect
huawei_B(protect-group-1)#protect-group enable
```

----End

Copyright © Huawei Technologies Co., Ltd.

13.3.4.9 Verifying Services

This topic describes how to verify the PRA PBX service by testing calls.

Prerequisites

The PRA PBX access service has been deployed.

Procedure

Step 1 Test calls between users connected to the PRA PBX according to table 1.

Step 2 Test calls from a user connected to the PRA PBX to an MGC user according to table 1.

Step 3 Test calls from an MGC user to a user connected to the PRA PBX according to table 1.

Table 13-9 PRA PBX access service verification

Category	Test Calls Between Users Connected to the PRA PBX	Test Calls from a User Connected to the PRA PBX to an MGC User	Test Calls from an MGC User to a User Connected to the PRA PBX
Prerequisites	1. User A and user B access the network through the PRA PBX and both users have been registered. 2. User A and user B are idle.	1. User A accesses the network through the PRA PBX and has been registered. 2. User B is a common MGC user and has been registered. 3. User A and user B are idle.	1. User A is a common MGC user and has been registered. 2. User B accesses the network through the PRA PBX and has been registered. 3. User A and user B are idle.
Test procedure	1. User A calls user B. 2. User B answers the call. Check the call between user A and user B. 3. User A releases the call.	The same as that in the "Test Calls Between Users Connected to the PRA PBX" column	The same as that in the "Test Calls Between Users Connected to the PRA PBX" column
Expected result	1. User B hears the ringing tone. 2. The call is set up. 3. The call is released.	The same as that in the "Test Calls Between Users Connected to the PRA PBX" column	The same as that in the "Test Calls Between Users Connected to the PRA PBX" column

----End

Copyright © Huawei Technologies Co., Ltd.

13.3.5 Enterprise E1 Unified Access Service

ONUs transmit E1 signals of enterprises to OLTs in SAToP mode and OLTs are interconnected with transmission equipment through E1 ports. In this manner, traditional circuit switching services can be carried over GPON networks.

13.3.5.1 Service Requirement and Application Scenario

Service Requirement

- Existing SDH resources are utilized efficiently. In this way, carriers' existing investments are protected and enterprise users in different regions are won.
- Services are received over optical fibers, reducing investment in copper cables between enterprises and the SDH network.
- The standardized user-side ports facilitate deployment and maintenance.

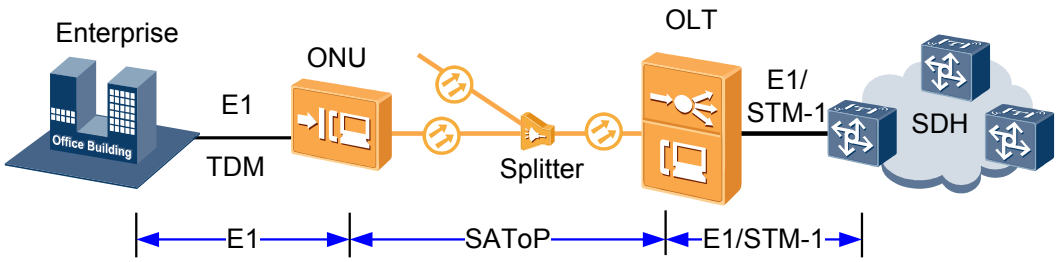
Application Scenario

As shown in **Figure 13-16**, the ONU accesses enterprise E1 service through standardized hardware ports, and transmits data to the OLT over the GPON line after performing structure-agnostic time division multiplexing over packet (SAToP) encapsulation on the service. After receiving the signals, the OLT restores E1 signals and transmits the signals to the SDH network.

- For carriers, with this networking, they can win enterprise users with GPON lines which support long-distance transmission and high bandwidth. With the trend of fiber-in and copper-out, deployment of GPON lines can reduce deployment costs of copper cables and support service expansion.
- For enterprise users, with GPON access, they can reduce fees spent in leasing lines.

ONUs supporting this scenario: MA5612, MA5628, MA5616.

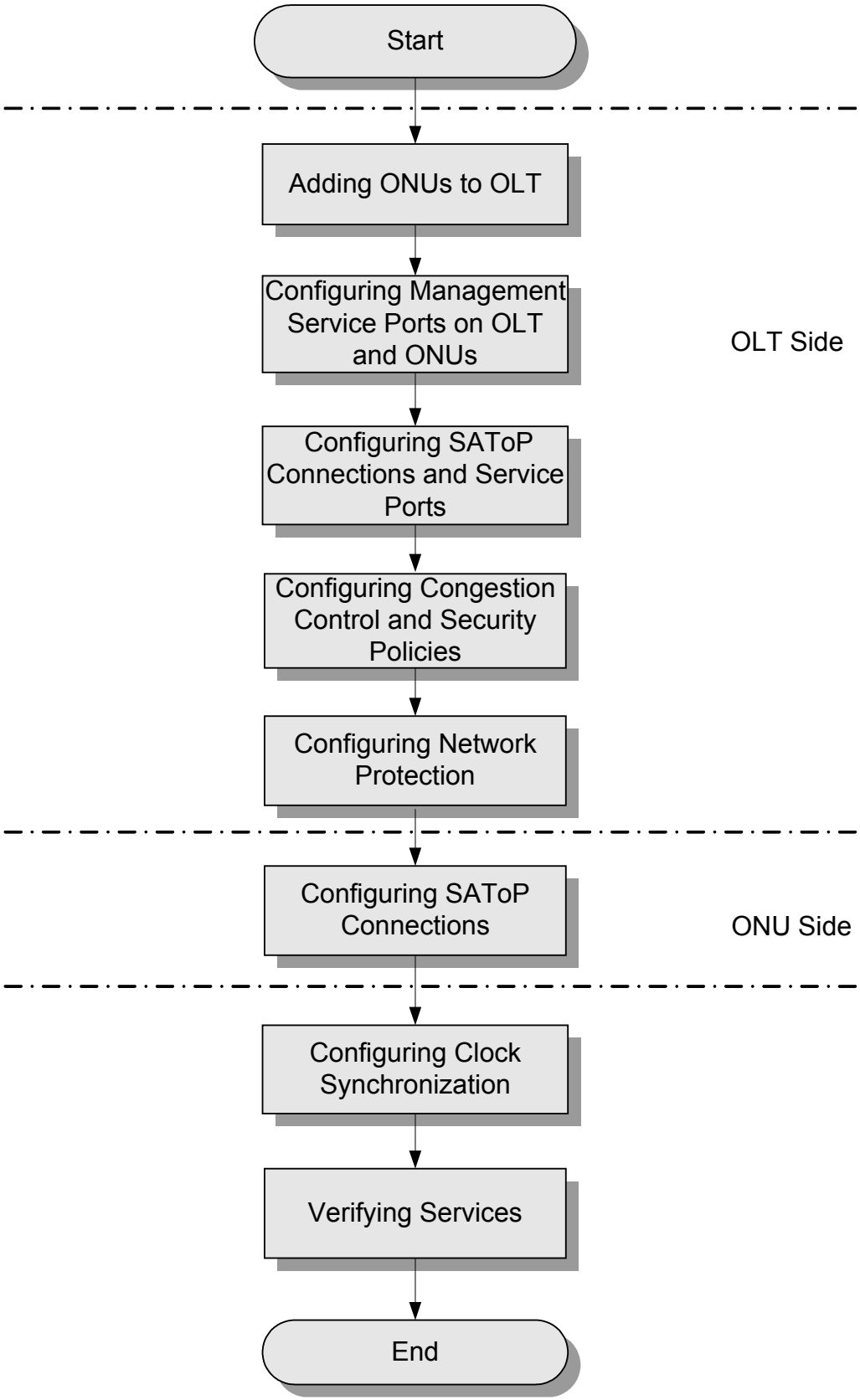
Figure 13-16 E1 access in SAToP mode



13.3.5.2 Configuration Process

The following figure shows the configuration process for E1/T1 enterprise private line.

Copyright © Huawei Technologies Co., Ltd.



Copyright © Huawei Technologies Co., Ltd.

13.3.5.3 Adding ONUs to OLT

ONUs can be configured only after they are added to the OLT successfully.

Context

- When adding ONUs, you need to bind related profiles to the ONUs, including the DBA profile, line profile, and alarm profile.
- An ONU can be added in two modes: offline addition and online confirmation. Select either mode as required.

Data Plan

Table 13-10 Key data plan

Item	Data
DBA profile	Profile ID: 20 Profile type: Fixed bandwidth and minimum delay DBA bandwidth: ● E1 access: 32 Mbit/s is recommended. (Each ONU accesses four E1 private lines and each line has a recommended DBA bandwidth of 8 Mbit/s) ● T1 access: 24 Mbit/s is recommended. (Each ONU accesses four T1 private lines and each line has a recommended DBA bandwidth of 6 Mbit/s)
Line profile	Profile ID: 10 T-CONT ID: 1 GEM port ID for management service: 11 GEM port ID for DDN private line service: 12
Networking data	PON port: 0/3/1 ONU parameters: ● ONU ID: 1 ● SN: 32303131B39FD641

Procedure

Step 1 Configure GPON ONU profiles.

1. Configure a DBA profile. and set the DBA bandwidth allocation mode for the GPON port to minimum bandwidth delay.

   For example, configure the DBA profile for 4-channel E1 private line.

```
huawei(config)#dba-profile add profile-id 20 type1 fix 32768
huawei(config)#interface gpon 0/3
huawei(config-if-gpon-0/3)#port dba bandwidth-assignment-mode 1 min-loop-delay
huawei(config-if-gpon-0/3)#quit
```


Copyright © Huawei Technologies Co., Ltd.

2. Configure an ONU line profile.

```
huawei(config)#ont-lineprofile gpon profile-id 10
huawei(config-gpon-lineprofile-10)#tcont 1 dba-profile-id 20  //Bind T-CONT 1
to DBA profile 20
huawei(config-gpon-lineprofile-10)#gem add 11 eth tcont 0
huawei(config-gpon-lineprofile-10)#gem add 12 eth tcont 1 //Add GEM port 12 to
T-CONT 1
huawei(config-gpon-lineprofile-10)#gem mapping 11 0 vlan 8
huawei(config-gpon-lineprofile-10)#gem mapping 12 1 vlan 300 //Map GEM port 12
to CVLAN 300
huawei(config-gpon-lineprofile-10)#commit
huawei(config-gpon-lineprofile-10)#quit
```

3. (Optional) Configure an alarm profile.
   - The default GPON alarm profile ID is 1. The value of each alarm threshold is **0** which indicates that alarms are not reported.
   - In this example, the default alarm profile is used and no configuration is required.

Step 2 Add ONUs to the OLT.

1. Add ONU 1 in offline mode.

```
huawei(config)#interface gpon 0/3
huawei(config-if-gpon-0/3)#ont add 1 ontid 1 sn-auth 32303131B39FD641
snmp ont-lineprofile-id 10
```

2. (Optional) Bind an alarm profile.

   By default, an ONU will be automatically bound to alarm profile 1 (default profile). You need to manually bind an alarm profile to an ONU only when the default alarm profile does not meet requirements.

   In this example, the default alarm profile is used. Therefore, you do not need to manually bind an alarm profile.

Step 3 Confirm the ONU status.

After adding an ONU, run the **display ont info** command to query the current status of the ONU. Ensure that **Control flag** is **active**, **Run State** is **online**, and **Config state** is **normal**.

The following uses ONU 1 as an example to describe how to confirm ONU status.

```
huawei(config-if-gpon-0/3)#display ont info 1 1
  ------------------------------------------------------------------------
  F/S/P                : 0/3/1
  ONT-ID               : 1
  Control flag         : active    //Indicates that the ONU is
activated.
  Run state            : online    //Indicates that the ONU is
online.
  Config state         : normal    //Indicates that the ONU is in normal
state.
...//Other command output is omitted.
huawei(config-if-gpon-0/3)#quit
```

----End

Follow-up Procedure

When **Config state** is **failed**, **Run state** is **offline**, or **Match state** is **mismatch**:

- If **Control flag** is **deactive**, run the **ont active** command in GPON mode to activate the ONU.

Copyright © Huawei Technologies Co., Ltd.

- If **Run state** is **offline**, a physical line may be broken or the optical module may be damaged. Check the line and the optical module.
- If **Config state** is **failed**, the configured ONU capability exceeds the actual ONU capability. In this case, run the **display ont failed-configuration** command in the diagnose mode to check the failed configuration item and the failure cause. Then, rectify the fault accordingly.
- If the ONU does not match, that is, **Match state** is **mismatch**, the port types and number of ports undermatch the actual port types and number of ports supported by the ONU. In this case, run the **display ont capability** command to query the actual capability of the ONU, and then select one of the following modes to modify the ONU configuration:
  - Create a proper ONU profile according to the actual capability of the ONU, and then run the **ont modify** command to modify the configuration data of the ONU.
  - Modify the ONU profile according to the actual capability of the ONU and save the modification. Then, the ONU automatically recovers the configuration successfully.

13.3.5.4 Configuring Management Service Ports on OLT and ONUs

This topic describes how to configure management service ports (also called service flows) on the OLT and ONUs. After the connections between the in-band management service ports on the OLT and ONUs are reachable, you can log in to the ONUs on the OLT and configure the ONUs.

Data Plan

Configuration Item	Data
Management VLAN and management IP address for OLT	Management VLAN ID: 8 Management VLAN type: smart In-band management IP address: 192.168.50.1/24
Management VLAN and management IP address for ONU	Management VLAN ID: 8 Management VLAN type: smart In-band management IP address for ONU 3: 192.168.50.2/24

Procedure

Step 1 Configure the in-band management VLAN and IP address for the OLT.

Set the in-band management VLAN to 8, VLAN priority to 6, and IP address to 192.168.50.1/24.

```
huawei(config)#vlan 8 smart
huawei(config)#port vlan 8 0/19 0
huawei(config)#vlan priority 8 6
huawei(config)#interface vlanif 8
huawei(config-if-vlanif8)#ip address 192.168.50.1 24
huawei(config-if-vlanif8)#quit
```

Step 2 Configure the in-band management VLAN and IP address for the ONU.

```
huawei(config)#interface gpon 0/3
huawei(config-if-gpon-0/3)#ont ipconfig 1 1 static ip-address 192.168.50.2 mask
```


Copyright © Huawei Technologies Co., Ltd.

```
255.255.255.0 gateway
192.168.50.1 vlan 8
huawei(config-if-gpon-0/3)#quit
```

Step 3 Configure the in-band management service port.

Set the management VLAN to 8, GEM port ID to 11, and user VLAN to 8. The OLT does not rate limit the in-band management service port. Therefore, directly use the default traffic profile 6.

```
huawei(config)#service-port vlan 8 gpon 0/3/1 ont 1 gemport 11 multi-service
user-vlan 8 rx-cttr 6 tx-cttr 6
```

Step 4 Confirm that the connection between the management service ports on the OLT and ONU is reachable.

- Run the **ping *ONU ip*** command on the OLT to verify the connectivity between the OLT and ONU. If the OLT receives ICMP ECHO-REPLY packets from the ONU, the connection is reachable.
- When the connection is reachable, you can remote log in to the ONU from the OLT and configure the ONU.

----End

13.3.5.5 Configuring SAToP Connections and Service Ports

This topic describes how to configure a SAToP connection of the IP+UDP encapsulation type and a service port to enable packets of enterprise to be encapsulated on ONUs and restored on OLTs.

Prerequisites

Required hardware is available:

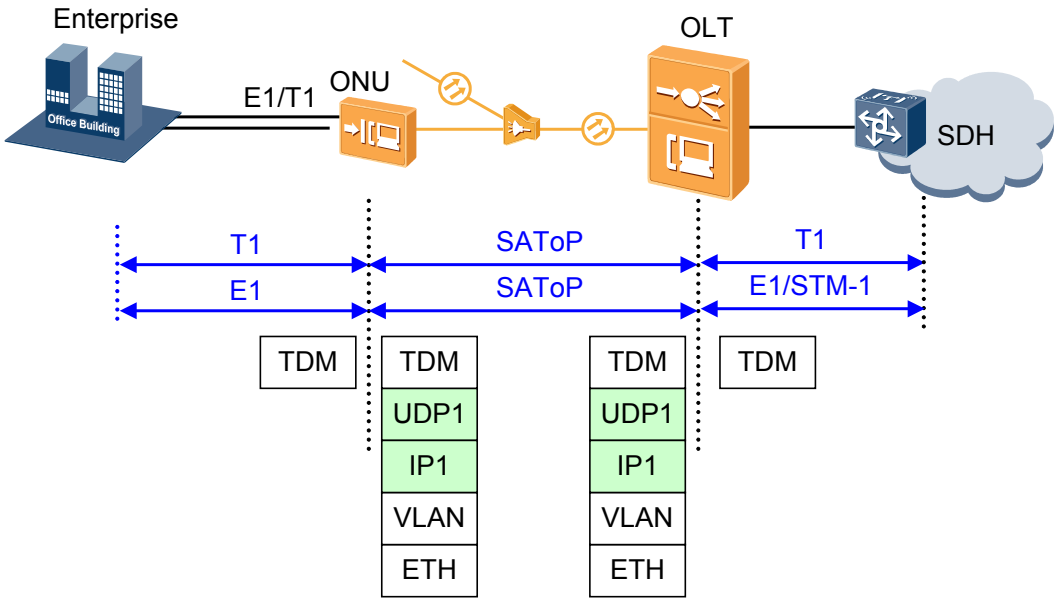
- Main control boards on the OLT: SCUN+CKMC/CKMD
- Upstream board on the OLT: EDTB (for E1 upstream transmission)
- Service board on the OLT: GPBD
- ONU: MA5612 (configured with the E81A board) or MA5628

Context

Figure 13-17 shows SAToP encapsulation for enterprise E1/T1 unified access service. As shown in the following figure, after TDM signals are encapsulated in the IP+UDP format, an outer VLAN tag and an Ethernet header are added to the TDM signals. Then the TDM signals become a standard Ethernet packet that is transmitted on the PON line between the ONU and OLT.

Copyright © Huawei Technologies Co., Ltd.

Figure 13-17 SAToP encapsulation



Data Plan

Configuration Item	Data
EDTB (OLT)	Port: 0/5/0 Board IP address: 10.10.50.10 Board MAC address: dynamically obtained (**remark 1**) Local UDP port number: 50048 (**remark 2**)
E1 port (ONU)	Board IP address: 10.10.50.20 Board MAC address: dynamically obtained (**remark 1**) UDP port number: 50048 (**remark 2**)
VLAN	SVLAN: 300

Remark 1: MAC address configuration modes (statically configured or dynamically obtained) at two ends must be consistent to establish a SAToP connection. It is recommended that MAC addresses be dynamically obtained, which facilitates configuration and maintenance.

Remark 2: The UDP port cannot be a port that is widely used in the industry and for specific services. For example, port 80 is used for HTTP service. The dynamic and private ports are recommended.

Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Configure EDTB board attributes.

Set the board working mode to SAToP.

```
huawei(config)#interface edt 0/5
huawei(config-if-edt-0/5)#board workmode satop
```

Configure the access mode and frame format.

- E1 access:
  ```
  huawei(config-if-edt-0/5)#tdm access-mode E1
  ```

Configure the IP address of the E1 port on the EDTB board.

```
huawei(config)#interface edt 0/5
huawei(config-if-edt-0/5)#set ip-address 10.10.50.10
huawei(config-if-edt-0/5)#quit
```

Step 2 Create a SAToP connection.

Create TDM VCL 10.

- For E1 access, set the TDM VCL type to SAToP.
  ```
  huawei(config)#tdm-vcl tdm-vcl-id 10 satop 0/5/0
  ```

Create a SAToP connection at the E1 port 0/5/0. Set SVLAN to 300, local UDP port number to 50048, remote IP address (the IP address of the E1 access board on the ONU) to 10.10.50.20, and remote UDP port number to 50048. The remote MAC address is obtained dynamically.

NOTE

To create a SAToP connection, the local UDP port number must be consistent with the remote UDP port number, that is, [*local-udp* = *portid* of EDTB + Cardinal number (50048)].

```
huawei(config)#cesop-connect tdm 10 vlan 300 local-udp 50048 remote-ip 10.10.50.20
remote-udp 50048
```

You can also create a SAToP connection by configuring the MAC address statically. If the remote MAC address (the MAC address of the E1 access board on the ONU, which can be queried by running the **display cesop-mac-address** command on the ONU) is 00e0-fc01-0450, create a SAToP connection in static mode as follows:

```
huawei(config)#cesop-connect tdm 10 vlan 300 local-udp 50048 remote-mac
 00e0-fc01-0450 remote-ip 10.10.50.20 remote-udp 50048
```

Step 3 (Optional) Configure attributes of the SAToP connection.

NOTE

The attributes of the SAToP connection on the OLT must be consistent with those on the ONU. Generally, use the system default values.

- Run the **cesop rtp** command to configure whether the SAToP packet carries the RTP header. The SAToP packet carries the RTP header by default.
- Run the **cesop encap** command to configure SSRC, payload type, and SN of the SAToP packet. The default value of these parameters is **0**.
- Run the **cesop jitter-buffer** command to configure the buffer depth of the SAToP packet. The default buffer depth is 2000 μs.
- Run the **cesop loadtime** command to configure the load time of the SAToP packet. The default load time is 125 μs.
- Run the **cesop priority** command to configure the priority of the SAToP packet. The default priority is 7.

Copyright © Huawei Technologies Co., Ltd.

Step 4 Configure a service port.

Set the service port ID to 1, SVLAN ID to 300, GEM port ID to 12, and user VLAN ID to 300. The ONU limits upstream and downstream traffic rates but the OLT does not. Therefore, use default traffic profile 6.

The user VLAN must be the same as the upstream VLAN of the ONU.

```
huawei(config)#vlan 300 smart
huawei(config)#service-port 1 vlan 300 gpon 0/3/1 ont 1 gemport 12 multi-service
user-vlan 300 rx-cttr 6 tx-cttr 6
```

----End

13.3.5.6 Configuring ONU SAToP Connections

This topic describes how to configure a SAToP connection of the IP+UDP encapsulation type and a service VLAN to enable packets of base stations to be encapsulated on ONUs as Ethernet packets and then forwarded based on VLANs and MAC addresses.

Data Plan

Configuration Item	Data
EDTB (OLT)	Port: 0/5/0 Board IP address: 10.10.50.10 Board MAC address: dynamically obtained (**remark 1**) Local UDP port number: 50048 (**remark 2**)
E1 port (ONU)	Board IP address: 10.10.50.20 Board MAC address: dynamically obtained (**remark 1**) UDP port number: 50048 (**remark 2**)
VLAN	SVLAN: 300

Remark 1: MAC address configuration modes (statically configured or dynamically obtained) at two ends must be consistent to establish a SAToP connection. It is recommended that MAC addresses be dynamically obtained, which facilitates configuration and maintenance.

Remark 2: The UDP port cannot be a port that is widely used in the industry and for specific services. For example, port 80 is used for HTTP service. The dynamic and private ports are recommended.

Procedure

Step 1 Configure a VLAN and add an upstream port to the VLAN.

Create the upstream VLAN 300, and add upstream port 0/0/1 to VLAN 300.

```
huawei(config)#vlan 300 smart
huawei(config)#port vlan 300 0/0 1
```


Copyright © Huawei Technologies Co., Ltd.

Step 2 Configure E1/T1 port attributes.

Configure the IP address of TDM service board 0/1 as 10.10.50.20.

```
huawei(config)#interface tdm 0/1
huawei(config-if-tdm-0/1)#set ip-address 10.10.50.20
```

Configure the board and port working mode and transmit clock.

- For E1 access, set the working mode to UDT and configure the transmit clock as the system clock.
  ```
  huawei(config-if-tdm-0/1)#tdm access-mode E1
  huawei(config-if-tdm-0/1)#port 0 udt system
  ```

Step 3 Create a SAToP connection.

Create TDM VCL 10.

- For E1 access, set the TDM VCL type to SAToP.
  ```
  huawei(config)#tdm-vcl tdm-vcl-id 10 satop 0/1/0
  ```

Create a SAToP connection at TDM port 0/1/0. Set SVLAN to 300, local UDP port number to 50048, remote IP address (the IP address of the EDTB board on the OLT) to 10.10.50.10, and remote UDP port number to 50048. The remote MAC address is obtained dynamically.

```
huawei(config)#cesop-connect tdm 10 vlan 300 local-udp 50048 remote-ip 10.10.50.10
remote-udp 50048
```

NOTE

You can also create a SAToP connection by configuring the MAC address statically. If the remote MAC address (the MAC address of the EDTB board on the OLT) is 0800-3E32-5310, create a SAToP connection in static mode as follows:

```
huawei(config)#cesop-connect tdm 10 vlan 300 local-udp 50048 remote-mac
 0800-3E32-5310 remote-ip 10.10.50.10 remote-udp 50048
```

Step 4 (Optional) Configure attributes of the SAToP connection.

NOTE

The attributes of the SAToP connection on the OLT must be consistent with those on the ONU. Generally, use the system default values.

- Run the **cesop rtp** command to configure whether the SAToP packet carries the RTP header. The SAToP packet carries the RTP header by default.
- Run the **cesop encap** command to configure SSRC, payload type, and SN of the SAToP packet. The default value of these parameters is **0**.
- Run the **cesop jitter-buffer** command to configure the buffer depth of the SAToP packet. The default buffer depth is 2000 μs.
- Run the **cesop loadtime** command to configure the load time of the SAToP packet. The default load time is 125 μs.
- Run the **cesop priority** command to configure the priority of the SAToP packet. The default priority is 7.

----End

13.3.5.7 Configuring Clock Synchronization

In this scenario, the E1/STM-1 line clock can be used to achieve network-wide clock synchronization.

Copyright © Huawei Technologies Co., Ltd.

Prerequisites

The CKMC/CKMD clock daughter board has been installed on the SCU main control board.

Context

Configuration roadmap for clock synchronization:

1. The OLT traces the upstream E1/STM-1 line clock of the TOPA board as the system clock.
2. The system clock is delivered to an ONU through optical paths of the GPON board.
3. The ONU uses the line clock of the GPON upstream port as the system clock.
4. The ONU E1 transmit clock is synchronized with the system clock of the ONU.

Procedure

- **Configure a clock on the OLT.**
  1. Add a system clock source.

     Configure the E1/T1 line clock input from port 0/5/0 on the EDTB board as the system clock 0. Set the priority to **0** (highest priority).

     ```
     huawei(config)#clock source 0 0/5/0
     huawei(config)#clock priority system 0
     ```

  2. Query configurations and the status of the system clock source.

     Run the **display clock source system** command to query configurations and the status of the clock source. Ensure that configurations of the system clock source are correct and the status is **Normal**.

     ```
     huawei(config)#display clock source system

     ------------------------------------------------------------------------
     -----
       Index  Board    Source   Clk-type  State       Priority QL
     Selected

     ------------------------------------------------------------------------
     -----
         0    H802EDTB 0/5/0    E1        Normal      0        ---
     YES

     ------------------------------------------------------------------------
     -----
     ```

     Run the **display clock mode** command to query the clock working mode. Ensure that the clock daughter board works in tracing mode.

     ```
     huawei(config)#display clock mode
       Clock manage-mode:Third-mode
       Clock subboard work-mode:Tracing
     ```

- **Configure a clock on the ONU.**
  1. Configure the GPON line clock as the system clock.

     The system clock of the OLT is delivered to the ONU through the GPON port on the OLT, achieving clock synchronization between the OLT and the ONU.

     a. Run the **clock source** command to configure the clock recovered from the GPON upstream port as the system clock of the ONU.

     b. Run the **clock priority** command to configure the priority of the clock source.

     ```
     huawei(config)#clock source 0 0/0/1
       Clock source set succeeded
     ```


Copyright © Huawei Technologies Co., Ltd.

```
huawei(config)#clock priority system 0
```

2. Configure the system clock as the transmit clock for an E1 port.
   a. Run the **interface tdm** command to enter the E1 port configuration mode.
   b. Run the **tx clock** or **port** *portid* **udt system** command to configure the system clock as the transmit clock of the port.
   c. Run the **display port state** command to query the transmit clock of the E1 port.

```
huawei(config)#interface tdm
huawei(config-if-tdm-)#port 0 udt system
huawei(config-if-tdm-)#display port state 0
  ---------------------------------------
  Port           : 0
  State          : normal
  Mode           : UDT
  Code           : HDB3
  Looptype       : -
  Timeslot       : -
  Clock          : system
  CRC4           : -
  Signaling      : -
  ESF            : -
  Impedance      : 120 Ohm
  ---------------------------------------
```

3. Query configurations and the status of the system clock source.
   Run the **display clock source** command to query configurations and the status of the system clock source.

```
huawei(config-if-tdm-)#quit
huawei(config)#display clock source
  ------------------------------------------------------------------
  Index  Config   Type   Source      State     Priority   Output
  ------------------------------------------------------------------
    0    YES      line   0/0/1       Normal    0          YES
    1    NO       --     -/ -/ -     ---       ---        ---
    2    NO       --     -/ -/ -     ---       ---        ---
    3    NO       --     -/ -/ -     ---       ---        ---
    4    NO       --     -/ -/ -     ---       ---        ---
    5    NO       --     -/ -/ -     ---       ---        ---
    6    NO       --     -/ -/ -     ---       ---        ---
    7    NO       --     -/ -/ -     ---       ---        ---
    8    NO       --     -/ -/ -     ---       ---        ---
    9    NO       --     -/ -/ -     ---       ---        ---
  ------------------------------------------------------------------
```

----End

13.3.5.8 Configuring Congestion Control and Security Policies

This topic describes how to configure global priority-based scheduling policies for queues to ensure service reliability and configure global security policies to ensure service security.

Context

Congestion control uses queue scheduling technology to map packets sent from the same port into multiple queues and process packets in each queue based on priority. Congestion control is recommended.

Security policies cover system security, user security, and service security, which ensure normal running of services.

Copyright © Huawei Technologies Co., Ltd.

NOTE

Enable security features based on service types. For details, see **13.2.5 Principle of Security Data Plan**.

Procedure

- Configure queue scheduling.

  Based on **13.2.3 Principle of QoS Data Plan**, all packets use strict priorities for queue scheduling and are mapped to queues based on priorities.

  ```
  huawei(config)#queue-scheduler strict-priority
  huawei(config)#cos-queue-map cos0 0 cos1 1 cos2 2 cos3 3 cos4 4 cos5 5 cos6 6 cos7 7  //System default
  ```

- Configure system security.
  - Enable deny of service (DoS) anti-attack on both the OLT and optical network units (ONUs).
    1. Run the **security anti-dos enable** command to globally enable DoS anti-attack.
    2. Run the **security anti-dos control-packet policy** command to configure a protocol packet processing policy that will be used when a DoS attack occurs.
    3. Run the **security anti-dos control-packet rate** command to configure the threshold for the rate of sending protocol packets to the CPU.
  - Enable IP address anti-attack on both the OLT and ONUs.

    Run the **security anti-ipattack enable** command to enable IP address anti-attack.
- Configure user security.
  - Enable MAC address anti-flapping on both the OLT and ONUs.

    Run the **security anti-macduplicate enable** command to enable MAC address anti-flapping.
  - Enable MAC address anti-spoofing on both the OLT and ONUs.
    1. In global config mode, run the **security anti-macspoofing enable** command to globally enable MAC address anti-spoofing.
    2. Enable MAC address anti-spoofing at VLAN level in global config mode or service profile mode:
       a. In global config mode, run the **security anti-macspoofing vlan** command to enable MAC address anti-spoofing.
       b. Perform the following operations to enable MAC address anti-spoofing in service profile mode:
          a. In global config mode, run the **vlan service-profile** command to create a VLAN service profile.
          b. Run the **security anti-macspoofing enable** command to enable MAC address anti-spoofing at VLAN level.
          c. Run the **commit** command to make the profile configuration take effect.
          d. Run the **quit** command to quit the VLAN service profile mode.
          e. Run the **vlan bind service-profile** command to bind the created VLAN service profile to a VLAN.
    3. (Optional) Run the **security anti-macspoofing max-mac-count** command to set the maximum number of MAC addresses that can be bound to a service flow.

Copyright © Huawei Technologies Co., Ltd.

4. (Optional) Run the **security anti-macspoofing exclude** command to configure the types of packets for which MAC address anti-spoofing does not take effect, such as Internet Group Management Protocol (IGMP) packets.

- Enable IP address anti-spoofing on ONUs.

  IP address anti-spoofing can be enabled or disabled at three levels: global, VLAN, and service port levels. This function takes effect only after it is enabled at the three levels. Among the three levels, IP address anti-spoofing is disabled only at the global level by default.

  1. In global config mode, run the **security anti-ipspoofing enable** command to enable IP address anti-spoofing at the global level.
  2. In VLAN service profile mode, run the **security anti-ipspoofing enable** command to enable IP address anti-spoofing at the VLAN level.
  3. Run the **security anti-ipspoofing service-port** *serviceport-id* **enable** command to enable IP address anti-spoofing at the service port level.

----End

13.3.5.9 Configuring Network Protectio

The base station access service has high requirements on reliability. Therefore, network protection solutions must be configured in the upstream and downstream directions.

Context

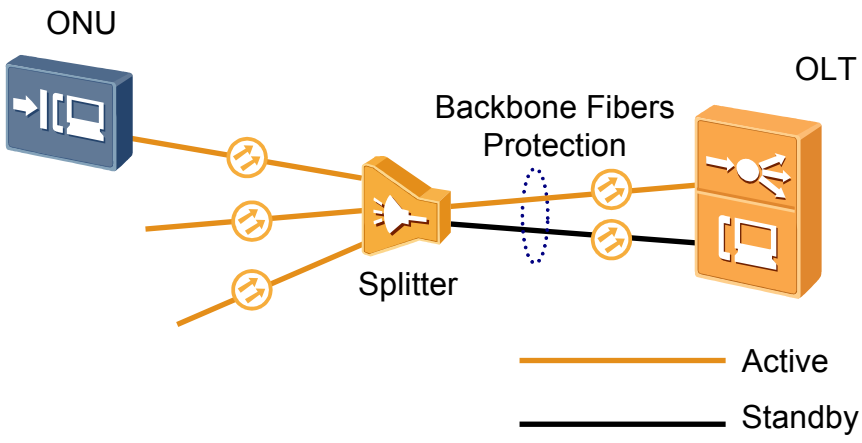
The protection solutions supported in this scenario are Type B protection and Type C single-homing protection.

Procedure

- Configure the Type B protection.

  Figure 13-18 shows the Type B protection networking diagram.

  Figure 13-18 Type B protection



  Configure redundancy backup for ports 0/3/1 and 0/3/2 on the same GPON board on OLT. When port 0/3/1 fails, the system can automatically switch to port 0/3/2.

Copyright © Huawei Technologies Co., Ltd.

```
huawei(config)#protect-group 0 protect-target gpon-uni-port workmode timedelay
huawei(protect-group-0)#protect-group member port 0/3/1 role work
huawei(protect-group-0)#protect-group member port 0/3/2 role protect
huawei(protect-group-0)#protect-group enable
```

NOTE

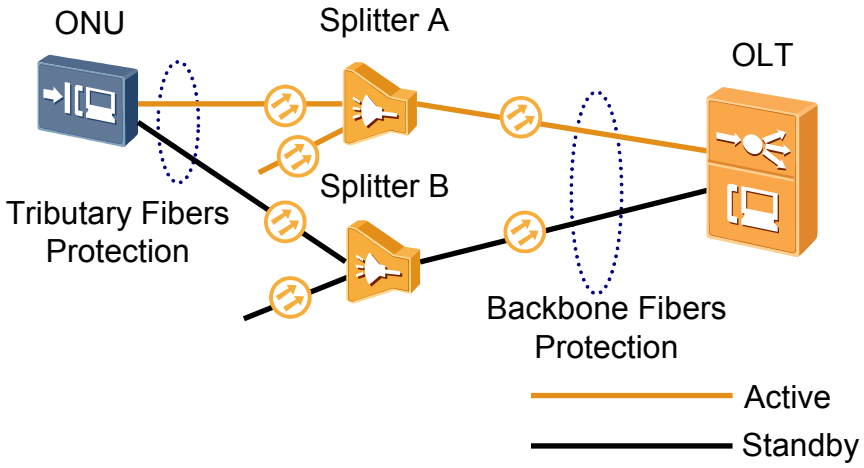
The configurations of services accessed by the ONUs remain the same after the Type B protection is configured. That is, the service configurations are applied only to the working GPON port.

- Configure the Type C single homing protection.

  Figure 13-19 shows networking diagram for the Type C single homing protection. Configure two 1:N optical splitters, one for connecting the working PON ports on the OLT and ONUs, and one for connecting the protection PON ports on the OLT and ONUs. This protection scheme protects both the backbone fibers and tributary fibers.

  The configurations of services accessed by the ONUs remain the same after the Type C single homing protection is configured. That is, the service configurations are applied only to the working PON port on the OLT and working upstream PON ports on the ONUs.

  Figure 13-19 Type C single homing protection



  As shown in the preceding figure, Type C single homing protecting is configured for optical fiber links between the OLT and ONU.

  - The ports on the GPON service board are 0/3/1 and 0/3/2.
  - The link at port 0/3/1 is the working link.
  - The link at port 0/3/2 is the protection link.
  - The ONU ID is 1.
  - The ONU is authenticated by serial number (SN). The SN of the ONU is 32303131B39FD641 and the management mode is SNMP.
  - The ID of the line profile bound to the ONU is 10.

```
huawei(config)#interface gpon 0/3
huawei(config-if-gpon-0/3)#ont add 1 1 sn-auth 32303131B39FD641 snmp ont-
lineprofile-id 10
huawei(config-if-gpon-0/3)#ont add 2 1 protect-side
huawei(config-if-gpon-0/3)#quit
huawei(config)#protect-group protect-target gpon-uni-ont workmode portstate
huawei(protect-group-1)#protect-group member port 0/3/1 ont 1 role work
huawei(protect-group-1)#protect-group member port 0/3/2 ont 1 role protect
```


Copyright © Huawei Technologies Co., Ltd.

```
huawei(protect-group-1)#protect-group enable
huawei(protect-group-1)#quit
```

----End

13.3.5.10 Verifying Services

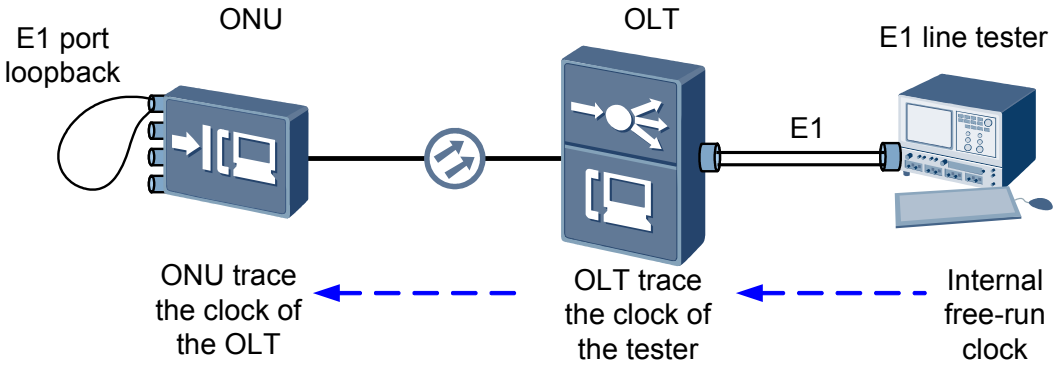
This topic describes how to use the PDH/SDH tester to verify the private line access service.

Prerequisites

The private line service has been configured.

Networking

Figure 13-20 Test setup for E1 upstream service



Procedure

Step 1 Set up network environment according to the preceding diagrams for service acceptance tests.

NOTE

Ensure clock synchronization for the test. It is recommended that the tester use the internal free-run clock, the OLT trace the clock of the tester, and the ONU trace the clock of the OLT.

Step 2 Use the E1 line tester to send packets for the test.

The test duration must be 12 hours or longer. There should be no alarms on the tester and the bit error rate must be less than 1E-9.

----End

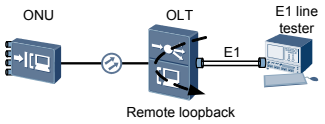
Follow-up Procedure

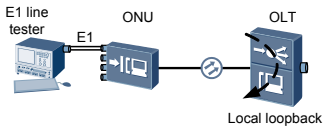
When the test on service connectivity fails, you can check for the failure causes by performing loopbacks. The following loopbacks are supported:

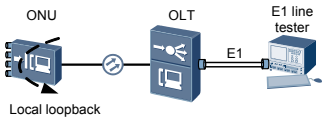
- Remote loopback on the OLT EDTB board
- Local loopback on the OLT EDTB board
- Local loopback on the ONU
- Remote loopback on the ONU

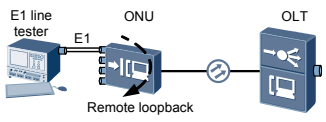
Copyright © Huawei Technologies Co., Ltd.

Loopback Mode	Function	Networking	Configuration

Remote loopback on the EDTB board	Loops back signals to the network side on the EDTB board on the OLT. This loopback checks whether the service from the EDTB board to the network-side channel is normal.		Enable/Disable the remote loopback for the E1 port.
			`huawei(config)#interface edt 0/5`
			`huawei(config-if-edt-0/5)#loopback 0 remote`
			`huawei(config-if-edt-0/5)#undo loopback 0`

Local loopback on the EDTB board	Loops back signals to the user side on the EDTB board on the OLT. This loopback checks whether the link between the EDTB board and the E1 port on the ONU is normal.		Enable/Disable the local loopback for the E1 port.
			`huawei(config)#interface edt 0/5`
			`huawei(config-if-edt-0/5)#loopback 0 local`
			`huawei(config-if-edt-0/5)#undo loopback 0`

Local loopback on the ONU	Loops back signals to the network side on the ONU. This loopback checks whether the link between the E1 port on the ONU and the EDTB board on the OLT is normal.		`huawei(config)#interface tdm`
			`huawei(config-if-tdm-)#loopback 0 local`
			`huawei(config-if-tdm-)#undo loopback 0`

Remote loopback on the ONU	Loops back signals to the user side on the ONU. This loopback checks whether the link between the ONU and user terminal is normal.		`huawei(config)#interface tdm`
			`huawei(config-if-tdm-)#loopback 0 remote`
			`huawei(config-if-tdm-)#undo loopback 0`

Copyright © Huawei Technologies Co., Ltd.

13.3.6 Enterprise E1/T1 Unified Access Service (OLT Cascading)

ONUs access enterprise TDM service in E1/T1 access mode, and transmits the data to the SDH network in OLT cascading mode over the GPON network which supports long-distance transmission and high bandwidth. In this way, uniform deployment of E1/T1 service is achieved.

13.3.6.1 Service Requirement and Application Scenario

Service Requirement

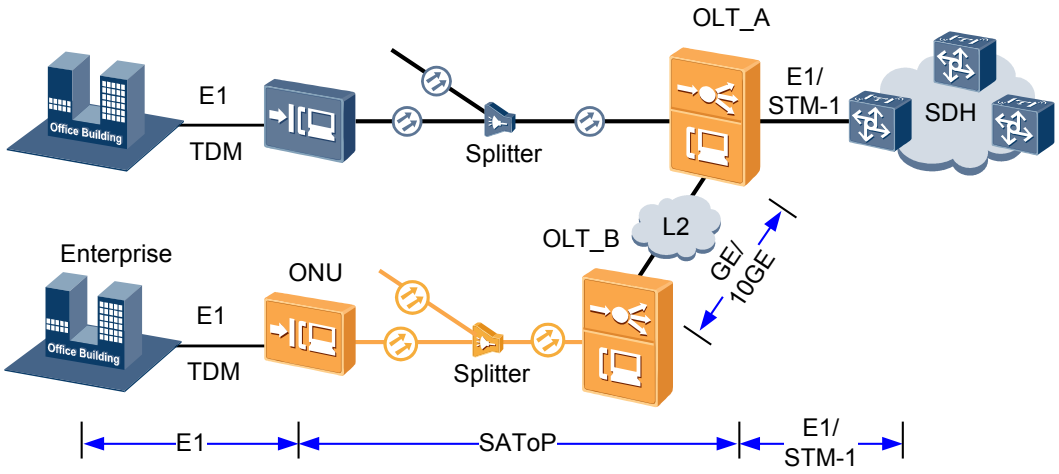
- Existing SDH resources are utilized efficiently. In this way, carriers' existing investments are protected and enterprise users in different regions are won.
- Services are received over optical fibers, reducing investment in copper cables between enterprises and the SDH network.
- The standardized user-side ports facilitate deployment and maintenance.

Application Scenario

As shown in **Figure 13-21**, a carrier's SDH network is migrated gradually. In a city, there are only some nodes (for example, OLT_A in the following figure) can transmit signals upstream to the SDH network through STM-1 ports, and other nodes (for example, OLT_B in the following figure) must access SDH resources through GE/10GE ports. In this scenario, ONU_B accesses the E1/T1 service in SAToP mode, and transmits the service to the OLT at the local site (OLT_B) over the GPON line. OLT_B transparently transmits the service to another OLT with SDH resources (OLT_A) through GE/10GE ports.

- For carriers, with this networking, they can win enterprise users who have no SDH resources with GPON lines which support long-distance transmission and high bandwidth. With the trend of fiber-in and copper-out, deployment of GPON lines can reduce deployment costs of copper cables and support service expansion.
- For enterprise users, with GPON access, they can reduce fees spent in leasing lines.

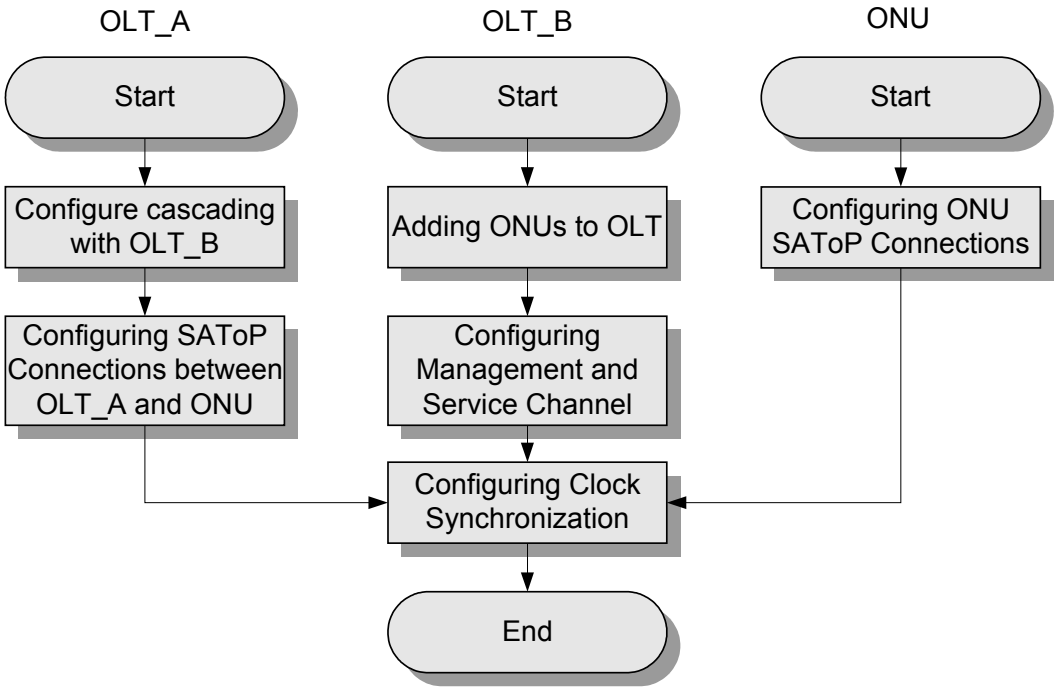
Figure 13-21 E1/T1 access in SAToP mode (OLT cascading)



Copyright © Huawei Technologies Co., Ltd.

13.3.6.2 Configuration Process

The following figure shows the configuration process for the E1/T1 unified access service (OLT cascading).



Functions of different network element are listed in the table below.

Network element	Functions
OLT_A	1. In the downstream direction, creates SAToP connections with ONU_B; in the upstream direction, restores E1/T1 signals and transmits the signals to the SDH network. 2. Cascaded with OLT_B and transmits clock synchronization information downstream.
OLT_B	1. Transmits SAToP-encapsulated packets in GEM frames over the GPON line. 2. Transmits SAToP packets to OLT_A in Ethernet mode for decapsulation. 3. Transmits clock synchronization information to ONU_B.
ONU_B	1. Access the E1/T1 private line service. 2. Create the SAToP connection between ONU_B and OLT_A. 3. Transmits SAToP packets to OLT_B by PON line. 4. Transmits clock synchronization information to enterprise.

Copyright © Huawei Technologies Co., Ltd.

13.3.6.3 Configure OLT_A cascading with OLT_B

Prerequisites

Required hardware for OLT_A is ready.

- Control board: SCUN+CKMC/CKMD
- GPON service board: GPBD
- Upstream board: EDTB
- Cascaded service board:
  - GE port: GICK or OPGD
  - 10GE port: X2CS

Data Plan

Table 13-11 provides the key data plan.

Table 13-11 Key data plan for OLT_A

Item	Data	Remarks
OPGD	Port: 0/2/1	Assume that OLT_A is cascaded with OLT_B using the OPGD board. Then you need to set the network role of the OPGD board to **cascade**.
VLAN ID and IP address	In-band management VLAN ID: 8 In-band management IP address: 192.168.50.30/24	To telnet to another OLT or ONU from the OLT and then configure the OLT or ONU, you must configure the in-band management VLANs and IP addresses of the OLT on the OLT. If the management IP address and the IP address of OLT_B or ONU_B are not in the same network segment, you also need to configure routes.

Procedure

Step 1 Configure the management VLAN and IP address.

Create management VLAN 8, and set the management IP address to 192.168.50.30 and subnet mask to 255.255.255.0.

```
huawei(config)#vlan 8 smart
huawei(config)#interface vlanif 8
huawei(config-if-vlanif8)#ip address 192.168.50.30 24
```

Step 2 Configure cascading with OLT_B.

Cascade OLT_A and OLT_B through GE port 0/2/1 on the OPGD board. Set the port attribute to **cascade**, and add the cascading port to VLAN 300.

```
huawei(config)#interface opg 0/2
huawei(config-if-opg-0/2)#network-role cascade
huawei(config-if-opg-0/2)#quit
```


Copyright © Huawei Technologies Co., Ltd.

```
huawei(config)#vlan 300 smart
huawei(config)#port vlan 300 0/2 1
```

----End

13.3.6.4 Configuring SAToP Connections between OLT_A and ONU

Data Plan

Configuration Item	Data
EDTB (OLT)	Port: 0/5/0 Board IP address: 10.10.50.10 Board MAC address: dynamically obtained (**remark 1**) Local UDP port number: 50048 (**remark 2**)
E1 port (ONU)	Board IP address: 10.10.50.20 Board MAC address: dynamically obtained (**remark 1**) UDP port number: 50048 (**remark 2**)
VLAN	SVLAN: 300

Remark 1: MAC address configuration modes (statically configured or dynamically obtained) at two ends must be consistent to establish a SAToP connection. It is recommended that MAC addresses be dynamically obtained, which facilitates configuration and maintenance.

Remark 2: The UDP port cannot be a port that is widely used in the industry and for specific services. For example, port 80 is used for HTTP service. The dynamic and private ports are recommended.

Procedure

Step 1 Configure EDTB board attributes.

Set the board working mode to SAToP.

```
huawei(config)#interface edt 0/5
huawei(config-if-edt-0/5)#board workmode satop
```

Configure the access mode and frame format.

- E1 access:
  ```
  huawei(config-if-edt-0/5)#tdm access-mode E1
  ```

Configure the IP address of the E1 port on the EDTB board.

```
huawei(config)#interface edt 0/5
huawei(config-if-edt-0/5)#set ip-address 10.10.50.10
huawei(config-if-edt-0/5)#quit
```

Step 2 Create a SAToP connection.

Create TDM VCL 10.

Copyright © Huawei Technologies Co., Ltd.

- For E1 access, set the TDM VCL type to SAToP.
  ```
  huawei(config)#tdm-vcl tdm-vcl-id 10 satop 0/5/0
  ```

Create a SAToP connection at the E1 port 0/5/0. Set SVLAN to 300, local UDP port number to 50048, remote IP address (the IP address of the E1 access board on the ONU) to 10.10.50.20, and remote UDP port number to 50048. The remote MAC address is obtained dynamically.

NOTE

To create a SAToP connection, the local UDP port number must be consistent with the remote UDP port number, that is, [*local-udp* = *portid* of EDTB + Cardinal number (50048)].

```
huawei(config)#cesop-connect tdm 10 vlan 300 local-udp 50048 remote-ip 10.10.50.20
remote-udp 50048
```

You can also create a SAToP connection by configuring the MAC address statically. If the remote MAC address (the MAC address of the E1 access board on the ONU, which can be queried by running the **display cesop-mac-address** command on the ONU) is 00e0-fc01-0450, create a SAToP connection in static mode as follows:

```
huawei(config)#cesop-connect tdm 10 vlan 300 local-udp 50048 remote-mac
 00e0-fc01-0450 remote-ip 10.10.50.20 remote-udp 50048
```

Step 3 (Optional) Configure attributes of the SAToP connection.

NOTE

The attributes of the SAToP connection on the OLT must be consistent with those on the ONU. Generally, use the system default values.

- Run the **cesop rtp** command to configure whether the SAToP packet carries the RTP header. The SAToP packet carries the RTP header by default.
- Run the **cesop encap** command to configure SSRC, payload type, and SN of the SAToP packet. The default value of these parameters is **0**.
- Run the **cesop jitter-buffer** command to configure the buffer depth of the SAToP packet. The default buffer depth is 2000 μs.
- Run the **cesop loadtime** command to configure the load time of the SAToP packet. The default load time is 125 μs.
- Run the **cesop priority** command to configure the priority of the SAToP packet. The default priority is 7.

----End

13.3.6.5 Adding ONUs to OLT_B

ONUs can be configured only after they are added to the OLT successfully.

Copyright © Huawei Technologies Co., Ltd.

Data Plan

Table 13-12 Key data plan

Item	Data
DBA profile	Profile ID: 20 Profile type: Fixed bandwidth and minimum delay DBA bandwidth: ● E1 access: 32 Mbit/s is recommended. (Each ONU accesses four E1 private lines and each line has a recommended DBA bandwidth of 8 Mbit/s) ● T1 access: 24 Mbit/s is recommended. (Each ONU accesses four T1 private lines and each line has a recommended DBA bandwidth of 6 Mbit/s)
Line profile	Profile ID: 10 T-CONT ID: 1 GEM port ID for management service: 11 GEM port ID for DDN private line service: 12
Networking data	PON port: 0/3/1 ONU parameters: ● ONU ID: 1 ● SN: 32303131B39FD641

Procedure

Step 1 Configure GPON ONU profiles.

1. Configure a DBA profile. and set the DBA bandwidth allocation mode for the GPON port to minimum bandwidth delay.

   For example, configure the DBA profile for 4-channel E1 private line.

```
huawei(config)#dba-profile add profile-id 20 type1 fix 32768
huawei(config)#interface gpon 0/3
huawei(config-if-gpon-0/3)#port dba bandwidth-assignment-mode 1 min-loop-delay
huawei(config-if-gpon-0/3)#quit
```

2. Configure an ONU line profile.

```
huawei(config)#ont-lineprofile gpon profile-id 10
huawei(config-gpon-lineprofile-10)#tcont 1 dba-profile-id 20  //Bind T-CONT 1 to DBA profile 20
huawei(config-gpon-lineprofile-10)#gem add 11 eth tcont 0
huawei(config-gpon-lineprofile-10)#gem add 12 eth tcont 1 //Add GEM port 12 to T-CONT 1
huawei(config-gpon-lineprofile-10)#gem mapping 11 0 vlan 8
huawei(config-gpon-lineprofile-10)#gem mapping 12 1 vlan 300 //Map GEM port 12 to CVLAN 300
huawei(config-gpon-lineprofile-10)#commit
huawei(config-gpon-lineprofile-10)#quit
```

3. (Optional) Configure an alarm profile.

Copyright © Huawei Technologies Co., Ltd.

- The default GPON alarm profile ID is 1. The value of each alarm threshold is **0** which indicates that alarms are not reported.
- In this example, the default alarm profile is used and no configuration is required.

Step 2 Add ONUs to the OLT.

1. Add ONU 1 in offline mode.

```
huawei(config)#interface gpon 0/3
huawei(config-if-gpon-0/3)#ont add 1 ontid 1 sn-auth 32303131B39FD641
snmp ont-lineprofile-id 10
```

2. (Optional) Bind an alarm profile.

   By default, an ONU will be automatically bound to alarm profile 1 (default profile). You need to manually bind an alarm profile to an ONU only when the default alarm profile does not meet requirements.

   In this example, the default alarm profile is used. Therefore, you do not need to manually bind an alarm profile.

Step 3 Confirm the ONU status.

After adding an ONU, run the **display ont info** command to query the current status of the ONU. Ensure that **Control flag** is **active**, **Run State** is **online**, and **Config state** is **normal**.

The following uses ONU 1 as an example to describe how to confirm ONU status.

```
huawei(config-if-gpon-0/3)#display ont info 1 1
  ------------------------------------------------------------------------
  F/S/P                : 0/3/1
  ONT-ID               : 1
  Control flag         : active    //Indicates that the ONU is
activated.
  Run state            : online    //Indicates that the ONU is
online.
  Config state         : normal    //Indicates that the ONU is in normal
state.
...//Other command output is omitted.
huawei(config-if-gpon-0/3)#quit
```

----End

Follow-up Procedure

When **Config state** is **failed**, **Run state** is **offline**, or **Match state** is **mismatch**:

- If **Control flag** is **deactive**, run the **ont active** command in GPON mode to activate the ONU.
- If **Run state** is **offline**, a physical line may be broken or the optical module may be damaged. Check the line and the optical module.
- If **Config state** is **failed**, the configured ONU capability exceeds the actual ONU capability. In this case, run the **display ont failed-configuration** command in the diagnose mode to check the failed configuration item and the failure cause. Then, rectify the fault accordingly.
- If the ONU does not match, that is, **Match state** is **mismatch**, the port types and number of ports undermatch the actual port types and number of ports supported by the ONU. In this case, run the **display ont capability** command to query the actual capability of the ONU, and then select one of the following modes to modify the ONU configuration:
  - Create a proper ONU profile according to the actual capability of the ONU, and then run the **ont modify** command to modify the configuration data of the ONU.

Copyright © Huawei Technologies Co., Ltd.

- Modify the ONU profile according to the actual capability of the ONU and save the modification. Then, the ONU automatically recovers the configuration successfully.

13.3.6.6 Configuring Management and Service Channel on OLT_B and ONU

After the management service ports is added, you can log in to the ONUs on the OLT and configure the ONUs. After the GPON service port is added, E1/T1 traffic stream are able to transmitted upstream to OLT_B.

Prerequisites

Required hardware for OLT_B (cascading) is ready.

- Control board: SCUN+CKMC/CKMD
- GPON service board: GPBD
- Upstream board:
  - GE port: GICK
  - 10GE port: X2CS

Data Plan

Item	Data
Management VLAN and management IP address for OLT	Management VLAN ID: 8 Management VLAN type: smart In-band management IP address: 192.168.50.1/24
Service VLAN	300
Management VLAN and management IP address for ONU	Management VLAN ID: 8 Management VLAN type: smart In-band management IP address: 192.168.50.2/24

Procedure

Step 1 Configure the in-band management VLAN and IP address for the OLT.

Set the in-band management VLAN to 8, VLAN priority to 6, and IP address to 192.168.50.1/24.

```
huawei(config)#vlan 8 smart
huawei(config)#port vlan 8 0/19 0
huawei(config)#vlan priority 8 6
huawei(config)#interface vlanif 8
huawei(config-if-vlanif8)#ip address 192.168.50.1 24
huawei(config-if-vlanif8)#quit
```

Step 2 Configure the in-band management VLAN and IP address for the ONU.

```
huawei(config)#interface gpon 0/3
huawei(config-if-gpon-0/3)#ont ipconfig 1 1 static ip-address 192.168.50.2 mask
255.255.255.0 gateway
192.168.50.1 vlan 8
huawei(config-if-gpon-0/3)#quit
```


Copyright © Huawei Technologies Co., Ltd.

Step 3 Configure the in-band management service port.

Set the management VLAN to 8, GEM port ID to 11, and user VLAN to 8. The OLT does not rate limit the in-band management service port. Therefore, directly use the default traffic profile 6.

```
huawei(config)#service-port vlan 8 gpon 0/3/1 ont 1 gemport 11 multi-service
user-vlan 8 rx-cttr 6 tx-cttr 6
```

Step 4 Confirm that the connection between the management service ports on the OLT and ONU is reachable.

- Run the **ping *ONU ip*** command on the OLT to verify the connectivity between the OLT and ONU. If the OLT receives ICMP ECHO-REPLY packets from the ONU, the connection is reachable.
- When the connection is reachable, you can remote log in to the ONU from the OLT and configure the ONU.

Step 5 Configure the upstream port.

Add upstream port 0/19/0 (on the GICK board) to VLAN 100.

```
huawei(config)#port vlan 100 0/19 0
```

Step 6 Configure the GPON service port.

Set SVLAN ID to 300, GEM port ID to 12, and CVLAN ID to 300. Rate limit for upstream and downstream packets is performed on the ONU instead of on the OLT. Therefore, use traffic profile 6 (default). To limit the rate of the service port, run the **traffic table ip** command to add a traffic profile and bind it to the service port.

The CVLAN must be the same as the upstream VLAN of the ONU.

```
huawei(config)#vlan 300 smart
huawei(config)#service-port vlan 300 gpon 0/3/1 ont 1 gemport 12 multi-service
user-vlan 300 rx-cttr 6 tx-cttr 6
```

----End

13.3.6.7 Configuring ONU SAToP Connections

This topic describes how to configure a SAToP connection of the IP+UDP encapsulation type and a service VLAN to enable packets of base stations to be encapsulated on ONUs as Ethernet packets and then forwarded based on VLANs and MAC addresses.

Data Plan

Configuration Item	Data
EDTB (OLT)	Port: 0/5/0 Board IP address: 10.10.50.10 Board MAC address: dynamically obtained (**remark 1**) Local UDP port number: 50048 (**remark 2**)

Copyright © Huawei Technologies Co., Ltd.

Configuration Item	Data
E1 port (ONU)	Board IP address: 10.10.50.20 Board MAC address: dynamically obtained (**remark 1**) UDP port number: 50048 (**remark 2**)
VLAN	SVLAN: 300

Remark 1: MAC address configuration modes (statically configured or dynamically obtained) at two ends must be consistent to establish a SAToP connection. It is recommended that MAC addresses be dynamically obtained, which facilitates configuration and maintenance.

Remark 2: The UDP port cannot be a port that is widely used in the industry and for specific services. For example, port 80 is used for HTTP service. The dynamic and private ports are recommended.

Procedure

Step 1 Configure a VLAN and add an upstream port to the VLAN.

Create the upstream VLAN 300, and add upstream port 0/0/1 to VLAN 300.

```
huawei(config)#vlan 300 smart
huawei(config)#port vlan 300 0/0 1
```

Step 2 Configure E1/T1 port attributes.

Configure the IP address of TDM service board 0/1 as 10.10.50.20.

```
huawei(config)#interface tdm 0/1
huawei(config-if-tdm-0/1)#set ip-address 10.10.50.20
```

Configure the board and port working mode and transmit clock.

- For E1 access, set the working mode to UDT and configure the transmit clock as the system clock.

```
huawei(config-if-tdm-0/1)#tdm access-mode E1
huawei(config-if-tdm-0/1)#port 0 udt system
```

Step 3 Create a SAToP connection.

Create TDM VCL 10.

- For E1 access, set the TDM VCL type to SAToP.

```
huawei(config)#tdm-vcl tdm-vcl-id 10 satop 0/1/0
```

Create a SAToP connection at TDM port 0/1/0. Set SVLAN to 300, local UDP port number to 50048, remote IP address (the IP address of the EDTB board on the OLT) to 10.10.50.10, and remote UDP port number to 50048. The remote MAC address is obtained dynamically.

```
huawei(config)#cesop-connect tdm 10 vlan 300 local-udp 50048 remote-ip 10.10.50.10
remote-udp 50048
```


Copyright © Huawei Technologies Co., Ltd.

NOTE

You can also create a SAToP connection by configuring the MAC address statically. If the remote MAC address (the MAC address of the EDTB board on the OLT) is 0800-3E32-5310, create a SAToP connection in static mode as follows:

```
huawei(config)#cesop-connect tdm 10 vlan 300 local-udp 50048 remote-mac
 0800-3E32-5310 remote-ip 10.10.50.10 remote-udp 50048
```

Step 4 (Optional) Configure attributes of the SAToP connection.

NOTE

The attributes of the SAToP connection on the OLT must be consistent with those on the ONU. Generally, use the system default values.

- Run the **cesop rtp** command to configure whether the SAToP packet carries the RTP header. The SAToP packet carries the RTP header by default.
- Run the **cesop encap** command to configure SSRC, payload type, and SN of the SAToP packet. The default value of these parameters is **0**.
- Run the **cesop jitter-buffer** command to configure the buffer depth of the SAToP packet. The default buffer depth is 2000 μs.
- Run the **cesop loadtime** command to configure the load time of the SAToP packet. The default load time is 125 μs.
- Run the **cesop priority** command to configure the priority of the SAToP packet. The default priority is 7.

----End

13.3.6.8 Configuring Clock Synchronization

Context

Configuration concept for clock synchronization:

1. OLT_A traces the upstream E1/T1 line clock of the EDTB board as the system clock.
2. OLT_B Obtains the system clock by GICK/X2CS boards in synchronous Ethernet mode.
3. The ONU uses the line clock of the GPON upstream port as the system clock.
4. The Tx clock of ONU is synchronized to the system clock of the ONU.

Data Plan

System clock	Clock source	Description
OLT_A	E1/T1 line clock: 0/5/0	OLT_A Obtains E1/STM-1 line clock from SDH as the system clock. and then transmits it to the cascading OLT_B over GE/10GE interface.
OLT_B	Synchronous ethernet line clock: 0/19/0	OLT_B Obtains the system clock in synchronous Ethernet mode. The clock is transmitted to the ONU over the GPON line.
ONU	GPON line clock: 0/0/1	ONU uses the line clock of the GPON upstream port as the system clock.

Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Cofnigure a clock on OLT_A.

1. Add a system clock source.

   Configure the E1/T1 line clock input from port 0/5/0 on the EDTB board as the system clock 0. Set the priority to **0** (highest priority).

```
huawei(config)#clock source 0 0/5/0
huawei(config)#clock priority system 0
```

2. Query configurations and the status of the system clock source.

   Run the **display clock source system** command to query configurations and the status of the clock source. Ensure that configurations of the system clock source are correct and the status is **Normal**.

```
huawei(config)#display clock source system

-------------------------------------------------------------------------------
  Index  Board    Source   Clk-type  State       Priority QL
Selected

-------------------------------------------------------------------------------
    0    H802EDTB 0/5/0    E1        Normal      0        ---
YES

-------------------------------------------------------------------------------
```

   Run the **display clock mode** command to query the clock working mode. Ensure that the clock daughter board works in tracing mode.

```
huawei(config)#display clock mode
  Clock manage-mode:Third-mode
  Clock subboard work-mode:Tracing
```

Step 2 Cofnigure a clock on OLT_B.

Obtain the system clock through the GICK board in synchronous Ethernet mode. The clock is transmitted to the ONU over the GPON line.

```
huawei(config)#clock source 0 0/19/0
huawei(config)#clock priority system 0
```

Step 3 Configure a clock on the ONU.

1. Configure the GPON line clock as the system clock.

   The system clock of the OLT is delivered to the ONU through the GPON port on the OLT, achieving clock synchronization between the OLT and the ONU.

   a. Run the **clock source** command to configure the clock recovered from the GPON upstream port as the system clock of the ONU.

   b. Run the **clock priority** command to configure the priority of the clock source.

```
huawei(config)#clock source 0 0/0/1
  Clock source set succeeded

huawei(config)#clock priority system 0
```

2. Configure the system clock as the transmit clock for an E1 port.

   a. Run the **interface tdm** command to enter the E1 port configuration mode.

Copyright © Huawei Technologies Co., Ltd.

b. Run the **tx clock** or **port** *portid* **udt system** command to configure the system clock as the transmit clock of the port.

c. Run the **display port state** command to query the transmit clock of the E1 port.

```
huawei(config)#interface tdm
huawei(config-if-tdm-)#port 0 udt system
huawei(config-if-tdm-)#display port state 0
  ---------------------------------------
  Port          : 0
  State         : normal
  Mode          : UDT
  Code          : HDB3
  Looptype      : -
  Timeslot      : -
  Clock         : system
  CRC4          : -
  Signaling     : -
  ESF           : -
  Impedance     : 120 Ohm
  ---------------------------------------
```

3. Query configurations and the status of the system clock source.

   Run the **display clock source** command to query configurations and the status of the system clock source.

```
huawei(config-if-tdm-)#quit
huawei(config)#display clock source
  ------------------------------------------------------------------
  Index  Config   Type   Source      State     Priority   Output
  ------------------------------------------------------------------
    0    YES      line   0/0/1       Normal    0          YES
    1    NO       --     -/ -/ -     ---       ---        ---
    2    NO       --     -/ -/ -     ---       ---        ---
    3    NO       --     -/ -/ -     ---       ---        ---
    4    NO       --     -/ -/ -     ---       ---        ---
    5    NO       --     -/ -/ -     ---       ---        ---
    6    NO       --     -/ -/ -     ---       ---        ---
    7    NO       --     -/ -/ -     ---       ---        ---
    8    NO       --     -/ -/ -     ---       ---        ---
    9    NO       --     -/ -/ -     ---       ---        ---
  ------------------------------------------------------------------
```

----End

13.3.6.9 Verifying Services

This topic describes how to use the PDH/SDH tester to verify the private line access service.

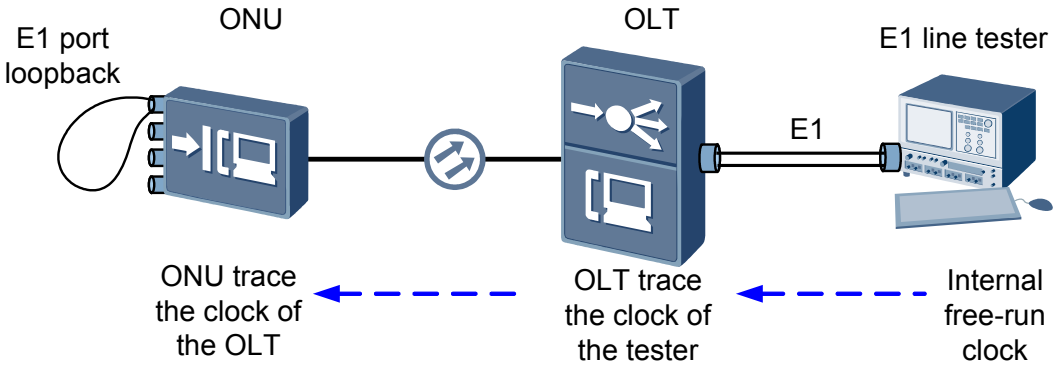
Prerequisites

The private line service has been configured.

Copyright © Huawei Technologies Co., Ltd.

Networking

Figure 13-22 Test setup for E1 upstream service



Procedure

Step 1 Set up network environment according to the preceding diagrams for service acceptance tests.

NOTE

Ensure clock synchronization for the test. It is recommended that the tester use the internal free-run clock, the OLT trace the clock of the tester, and the ONU trace the clock of the OLT.

Step 2 Use the E1 line tester to send packets for the test.

The test duration must be 12 hours or longer. There should be no alarms on the tester and the bit error rate must be less than 1E-9.

----End

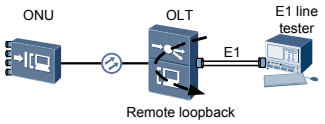
Follow-up Procedure

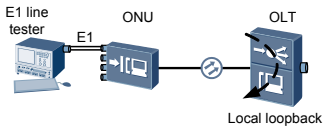
When the test on service connectivity fails, you can check for the failure causes by performing loopbacks. The following loopbacks are supported:

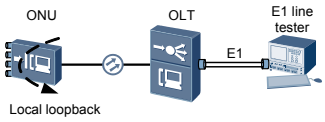
- Remote loopback on the OLT EDTB board
- Local loopback on the OLT EDTB board
- Local loopback on the ONU
- Remote loopback on the ONU

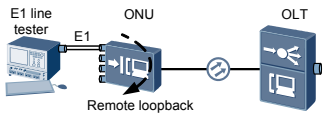
Copyright © Huawei Technologies Co., Ltd.

Loopback Mode	Function	Networking	Configuration

Remote loopback on the EDTB board	Loops back signals to the network side on the EDTB board on the OLT. This loopback checks whether the service from the EDTB board to the network-side channel is normal.		Enable/Disable the remote loopback for the E1 port.
			`huawei(config)#interface edt 0/5`
			`huawei(config-if-edt-0/5)#loopback 0 remote`
			`huawei(config-if-edt-0/5)#undo loopback 0`

Local loopback on the EDTB board	Loops back signals to the user side on the EDTB board on the OLT. This loopback checks whether the link between the EDTB board and the E1 port on the ONU is normal.		Enable/Disable the local loopback for the E1 port.
			`huawei(config)#interface edt 0/5`
			`huawei(config-if-edt-0/5)#loopback 0 local`
			`huawei(config-if-edt-0/5)#undo loopback 0`

Local loopback on the ONU	Loops back signals to the network side on the ONU. This loopback checks whether the link between the E1 port on the ONU and the EDTB board on the OLT is normal.		`huawei(config)#interface tdm`
			`huawei(config-if-tdm-)#loopback 0 local`
			`huawei(config-if-tdm-)#undo loopback 0`

Remote loopback on the ONU	Loops back signals to the user side on the ONU. This loopback checks whether the link between the ONU and user terminal is normal.		`huawei(config)#interface tdm`
			`huawei(config-if-tdm-)#loopback 0 remote`
			`huawei(config-if-tdm-)#undo loopback 0`

Copyright © Huawei Technologies Co., Ltd.

14 FTTM Configuration (Base Station Access)

About This Chapter

On a FTTM (base station access) network, 2G or 3G/4G base stations are connected to ONUs that serve as cell backhaul units (CBUs) in multiple modes. Then the ONUs transmit 2G or 3G services to OLTs and then to the upper-layer network. After being transmitted over the upper-layer network, the services access the basic station controller (BSC) or radio network controller (RNC). In this manner, 2G or 3G services are carried on the base station access network.

14.1 Overview of Base Station Access Service
Before configuring the base station access service, acquire the following basic knowledge.

14.2 Prinpicle of Planning Data for Base Station Access Service
This topic plans base station access service in a unified manner from different dimensions. The data plans are used to guide configuration and optimization of base station access service in different scenarios.

14.3 Configuring Base station access Clock Synchronization
This topic describes the concept and principle of clock synchronization in bse station access network, clock synchronization solutions supported by devices, and configuration differences.

14.4 Configuring Base Station Access Service (GPON)
This topic describes how to configure the base station access service in GPON mode in different networking scenarios.

Copyright © Huawei Technologies Co., Ltd.

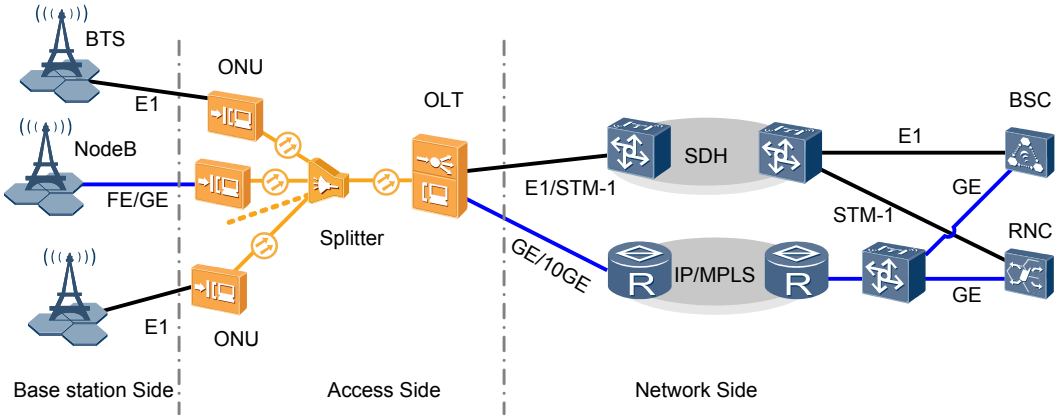
14.1 Overview of Base Station Access Service

Before configuring the base station access service, acquire the following basic knowledge.

14.1.1 Basic Concepts

Many concepts are involved in the base station access solution. The following only provides major concepts involved in the network diagram of base station access service.

Network Diagram of Base Station Access Service



User Side

Concept	Description
BTS	Base transceiver station, a 2G base station. BTSs are controlled by base station controllers (BSCs) and constitute a a base station subsystem (BSS) with BSCs as radio devices. BTSs serve for a district and communicate with mobile stations (MSs) through air interfaces.
NodeB	A 3G base station, providing physical radio links between mobile devices (mobile phones) and the universal mobile telecommunications system (UMTS) network. NodeBs transmit and receive data through radio interfaces.

Copyright © Huawei Technologies Co., Ltd.

Network Side

Concept	Description
SDH	Synchronous digital hierarchy. SDH is a transmission scheme that follows ITU-T G.707, G.708, and G.709. It defines the transmission features of digital signals such as frame structure, multiplexing mode, transmission rate level, and interface code. SDH is an important part of ISDN and B-ISDN. It interleaves the bytes of low-speed signals to multiplex the signals to high-speed counterparts, and the line coding of scrambling is used only for signals. SDH is suitable for the fiber communications system with high speed and a large capacity since it uses synchronous multiplexing and flexible mapping structure.
PTN	Packet transport network. PTN provides bidirectional point-to-point connections for packet switching services and supports point-to-point networking using various service granularities. It can use lower-layer transmission channels such as SDH, Ethernet, and OTN to transmit services.
BSC/RNC	BSC: Base station controller. A BSC controls a group of base stations and manages the radio network. Specifically, BSCs manage radio districts and channels, operate and maintain radio devices, manage connections of MSs, and provide interfaces between base stations and the mobile switching center (MSC). Radio control functions can be integrated in BSCs whenever possible to simplify functions of base stations. RNC: radio network controller. RNCs are key NEs on 3G networks. RNCs manage mobility, process calls, manage links, and switch users on the access network.

14.1.2 Networking Scenarios and Hardware Configurations (GPON)

This topic provides typical networking scenarios for base station access service and typical hardware configurations of OLTs and ONUs based on locations and types of ONUs.

Copyright © Huawei Technologies Co., Ltd.

Typical Networking Scenarios and Hardware Configurations for Base Station Access Service (GPON)

Scenario	Description	Typical OLT Configuration (Main Control Board+Service Board +Upstream Board)	Applicable ONU
E1 base station access service (in Native TDM mode)	the ONU accesses TDM services of the 2G or 3G base station through the E1 port, and then transmits the service data to the GPON service board on the OLT in the Native TDM mode. The OLT restores TDM signals, and then transmits the signals to the SDH network through the E1 port (provided by the NH1A daughter board) or STM-1 port (provided by the O2CE daughter board) on the TOPA board. In this manner, service access of the 2G or 3G base station is implemented between the ONU and the OLT in the Native TDM mode.	SCUN+GPBC/ GPBD+TOPA ● E1 upstream transmission: The daughter board for TOPA is NH1A. ● STM-1 upstream transmission: The daughter board for TOPA is O2CE.	MA5612, MA5628
E1 base station access service (in SAToP mode)	the ONU accesses E1/T1 services of the 2G or 3G base station through the unified hardware port, and then transmits the service data to the OLT in the SAToP mode. The OLT restores E1/T1 signals, and then transmits the signals to the SDH network through the E1/T1 port. In this manner, service access of the 2G or 3G base station is implemented between the ONU and the OLT in the SAToP mode.	SCUN+GPBC/ GPBD+EDTB	MA5612, MA5628

Copyright © Huawei Technologies Co., Ltd.

Scenario	Description	Typical OLT Configuration (Main Control Board+Service Board +Upstream Board)	Applicable ONU
Ethernet base station access service (in QinQ VLAN mode)	ONUs receive the ETH service data from 3G base stations through FE/GE ports, encapsulate the ETH packets into GEM frames, and then send them to the OLT through the GPON upstream ports. The OLT restores the ETH signals and configures QinQ VLANs for the signals to enable the data of base stations to be transparently transmitted to the remote PTN over the public network. Then the remote PTN device restores the ETH signals.	SCUN+GPBC/ GPBD+GICK/ X2CS	MA5612, MA5628

14.1.3 GPON ONU Capability Set

This topic describes the supported hardware capability, features, and network position of ONUs on a GPON FTTM access network.

In FTTx V100R013C00, the MA5694S, MA5698, MA5898, MA5612, MA5628 and MA5673 mainly apply to the FTTM access service. **Table 14-1** shows the ONU capability set.

Table 14-1 ONU capability set

ONU Type	User Interface	Supported ONU Version
MA5694S	As an outdoor box-type device, MA5694S is used for data backhaul of small cell base stations. It provides the following interfaces: ● 1*GE optical interface for Ethernet access ● 3*GE electrical interfaces for Ethernet access, power on Ethernet is supported ● 1*GPON interface for upstream	V800R313C10

Copyright © Huawei Technologies Co., Ltd.

ONU Type	User Interface	Supported ONU Version
MA5698	Typical configuration: ● Pure broadband configurations: supports 4xGE interfaces+16xFE electrical interfaces when two EIUC boards are configured ● Leased line access configurations: supports 16xE1 interfaces when two E81A boards are configured	V800R313C00
MA5898	Typical configuration: ● Pure broadband configurations: supports 4xGE interfaces+16xFE electrical interfaces when two EIUC boards are configured ● Leased line access configurations: supports 16xE1 interfaces when two E81A boards are configured	V800R313C00
MA5612	For the bottom plate with POTS ports: ● Supports 2xGE electrical interfaces+6xFE electrical interfaces+48xPOTS interfaces+(optional)1xRF interface when two ASNB boards are configured. ● Supports 2xGE electrical interfaces+22xFE electrical interfaces+16xPOTS interfaces+(optional) 1xRF interface when two EIUC boards are configured. ● Supports 2xGE electrical interfaces+6xFE electrical interfaces+16xE1/T1 interfaces+16xPOTS interfaces+(optional)1xRF interface when two E81A boards are configured. For the bottom plate without POTS ports: ● Supports 2xGE electrical interfaces+6xFE electrical interfaces+32xPOTS interfaces when two ASNB boards are configured. ● Supports 2xGE electrical interfaces+22xFE electrical interfaces when two EIUC boards are configured. ● Supports 2xGE electrical interfaces+6xFE electrical interfaces+16xE1/T1 interfaces when two E81A boards are configured.	● V800R308C00 ● V800R308C01 ● V800R310C00 ● V800R311C00 ● V800R312C00
MA5628	There are two types of MA5628: integrated and box-type. Both integrated MA5628 and box-type MA5628 provide: ● 4xE1/T1 interfaces ● 4xGE electrical interfaces	● V800R308C01 ● V800R309C00 ● V800R310C00 ● V800R311C00 ● V800R312C00

Copyright © Huawei Technologies Co., Ltd.

ONU Type	User Interface	Supported ONU Version
MA5673	As a "bridge + Voice" type of ONU, MA5673 provides the following interfaces: ● 4*GE interfaces for Ethernet access ● 4*POTS interfaces for VoIP access ● 4*E1 interfaces for E1 Native TDM leased line access	V800R313C00

14.2 Prinpicle of Planning Data for Base Station Access Service

This topic plans base station access service in a unified manner from different dimensions. The data plans are used to guide configuration and optimization of base station access service in different scenarios.

14.2.1 Principle of Equipment Management Data Plan

Equipment management planning involves planning for management VLANs and IP addresses.

Management VLAN Planning

- The OLT and ONUs use the same management VLAN.
- The OLT and ONUs use a single SVLAN as the equipment management VLAN.

IP Address Planning

Scenario	IP Address Planning
Equipment management	A management IP address is allocated to each OLT/ONU. Management IP addresses of ONUs connected to the same OLT are usually in the same network segment. Private IP addresses planned by the carrier are used for the purpose of security.
E1 base station access service (in Native TDM mode)	No IP addresses need to be planned because ONUs access the private line service through E1.
E1/T1 base station access service (in SAToP mode)	IP addresses are planned as follows: ● On OLTs, source IP addresses of SAToP connections must be planned for EDTB boards. ● On ONUs, source IP addresses of SAToP connections must be planned for E1 boards. These IP addresses are valid only between OLTs and ONUs and therefore can be planned as private IP addresses.

Copyright © Huawei Technologies Co., Ltd.

Scenario	IP Address Planning
Ethernet base station access service (in QinQ VLAN mode)	No IP addresses need to be planned because the OLT and ONUs provide Layer 2 transparent channels.

14.2.2 Principle of VLAN Data Plan

VLAN planning for the base station access service covers planning of VLANs and VLAN translation policies in different networking scenarios.

VLAN and VLAN Translation Policy

Scenario	VLAN Planning	VLAN Translation	
		ONU	OLT
E1 base station access service (in Native TDM mode)	Use a reserved CVLAN (starts from 4000). **NOTICE** A reserved CVLAN cannot be used for Ethernet services on ONUs.	N/A	N/A
E1/T1 base station access service (in SAToP mode)	Plan a global VLAN on the OLT and ONUs, which cannot conflict with other service VLANs.	N/A	N/A

Copyright © Huawei Technologies Co., Ltd.

Scenario	VLAN Planning	VLAN Translation	
		ONU	OLT
Ethernet base station access service (in QinQ VLAN mode)	Single VLAN tag: ONUs and the OLT use single VLAN tags. Service packets are forwarded based on single VLAN tags after being transmitted from the OLT upstream to the metro network. In this way, a large number of VLANs for the metro network will be occupied if there are many OLTs. Generally, four VLANs are planned for Ethernet base station access service, which are used for: ● Clock synchronization ● Voice and data services of base stations ● Base station management ● ONU management	1. Different user VLANs are planned for different services (service packets with different destination addresses or paths) of base stations. 2. User VLANs of packets sent from the base stations are translated to a specified CVLAN based on service types.	The OLT transparently transmits packets with CVLANs from ONUs.
	(Recommended) Double VLAN tags: Each OLT uses double VLAN tags, an outer VLAN tag (SVLAN) and inner VLAN tag (CVLAN). SLVANs are the same but CLVANs are different. In this way, the number of VLANs required for the metro network is significantly reduced.	1. Different user VLANs are planned for different services (service packets with different destination addresses or paths) of base stations. 2. User VLANs of packets sent from the base stations are translated to a specified CVLAN based on service types.	The OLT adds an SVLAN tag: CVLAN<->SVLAN +CVLAN.

Copyright © Huawei Technologies Co., Ltd.

14.2.3 Principle of QoS Data Plan

QoS planning for the base station access service is end-to-end. QoS policies include traffic classification, marking and scheduling, traffic monitoring, and DBA policies. QoS policies for different scenarios are different. This topic provides QoS policies in the following scenarios.

E1 Base Station Access Service (in Native TDM Mode)

In this scenario, ONUs access services through E1 lines. Therefore, the QoS policies are mainly planned for traffic on PON lines.

Parameter	Value	Remarks
T-CONT	It is recommended that the number of T-CONTs do not exceed 3. The T-CONT ID ranges from 1 to 3.	It is recommended that all E1 lines of the same ONU use the same T-CONT.
DBA type	Fixed bandwidth and minimum delay	The DBA must be configured properly to achieve low delay, low jitter, and zero packet loss so that the quality of the E1 base station access service can be ensured.
DBA bandwidth	Nx7232 kbit/s is recommended. (N is the number of E1 lines.)	It is recommended that the T-CONT ID be 1, 2, or 3 and all E1 lines of the same ONU use the same T-CONT. This setting can leverage bandwidth resources. Each E1 line requires only 5440 kbit/s.

E1/T1 Base Station Access Service (in GPON SAToP Mode)

In this scenario, ONUs access services through E1/T1 lines. Therefore, the QoS policies are mainly planned for traffic on PON lines.

Parameter	Value	Remarks
T-CONT	It is recommended that the number of T-CONTs do not exceed 3. The T-CONT ID ranges from 1 to 3.	It is recommended that all E1 lines of the same ONU use the same T-CONT.
DBA type	Fixed bandwidth and minimum delay	The DBA must be configured properly to achieve low delay, low jitter, and zero packet loss so that the quality of the T1 base station access service can be ensured.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Value	Remarks
DBA bandwidth	● E1 access: Nx8 Mbit/s is recommended. (N is the number of E1 lines.) ● T1 access: Nx6 Mbit/s is recommended. (N is the number of E1 lines.)	-

Ethernet Base Station Access Service (in QinQ VLAN Mode)

Parameter			Value
Traffic classification, marking, and scheduling policies		802.1p priority	OAM service of base stations: 7 Synchronization service of base stations: 7 Voice and data services of base stations: 7
		Queue scheduling mode	PQ
		OLT queue ID (eight queues)	7
Traffic monitoring and DBA policies	OLT	T-CONT (only for GPON)	QinQ private line services use a separate T-CONT to distinguish the QinQ private line services from other services.
		DBA type	Type 3 ("Assured bandwidth+maximum bandwidth" DBA profile. This type of DBA not only ensures a fixed bandwidth for users but also enables users to preempt a certain amount of bandwidth, but the total bandwidth cannot exceed the maximum bandwidth.)
		DBA bandwidth	Configure DBA bandwidth based on bandwidth requirements of base stations.
		Downstream traffic profile	Configure a traffic profile based on bandwidth requirements of base stations.
	ONU	Upstream port rate limit	Rates of upstream ports are not limited.
		Downstream port rate limit	Rates of downstream ports are not limited.

14.2.4 Principle of Clock Synchronization Data Plan

Wireless base stations have high requirements on clock precision. Clock synchronization solutions must be planned based on types and standards of base stations.

Copyright © Huawei Technologies Co., Ltd.

Clock Synchronization Solution

Classification	Clock Synchronization Solution	Description
Frequency synchronization	BITS clock	For GSM and WCDMA base stations that only require frequency synchronization, BITS clocks are transmitted to base stations to achieve network-wide clock synchronization when OLTs have BITS input clocks.
	E1/STM-1 line clock	For GSM and WCDMA base stations that only require frequency synchronization, E1/STM-1 line clocks are used to achieve clock synchronization when OLTs transmit services upstream to SDH networks through E1/STM-1 ports.
	Synchronous Ethernet clock	For GSM and WCDMA base stations that only require frequency synchronization, clocks restored from code streams on Ethernet links are used to achieve network-wide clock synchronization when OLTs transmit services upstream to PSN networks through GE/10GE ports.
Time synchronization	1PPS+ToD time	OLTs receive time information through 1PPS+TOD ports. The time information is transmitted from external time servers (such as Huawei SYNLOCK T6020) that obtain standard time synchronization information using GPS. This solution is recommended for 3G and LTE stations.
	1588V2 time	The OLT obtains the 1588v2 time by using the upstream network interface (the time is transmitted by the upstream network hop by hop). Then, the OLT transmits the time to the ONU through the GPON line. After recovering the time, the ONU transmits the time to the base station by means of the 1588v2 or time interface.

NOTE

The priority of recommended frequency synchronization solutions is as follows: BITS clock > line clock > synchronous Ethernet clock. Select a clock source based on the actual conditions of COs.

Recommended Clock Synchronization Solutions for Different Base Station Access Scenarios

Scenario	Recommended Clock Synchronization Solution
E1 base station access service (in Native TDM mode)	BITS clock E1/STM-1 line clock
T1 base station access service (in GPON SAToP mode)	BITS clock E1/STM-1 line clock

Copyright © Huawei Technologies Co., Ltd.

Scenario	Recommended Clock Synchronization Solution
Ethernet base station access service (in QinQ VLAN mode)	Synchronous Ethernet clock 1PPS+ToD time (remark 1) 1588v2 time

Remark 1: Ethernet base stations may require time synchronization.

14.2.5 Principle of Security Data Plan

Security planning involves planning for system security, user security, and service security. Security policy ensures normal services.

NOTE

- The device provides complete security measures, but not all security measures need to be deployed. Only the security measures that meet the following requirements need to be deployed:
  - The security measures can be used on the live network.
  - The security measures are easy to deploy.
  - The security measures are effective.
- Different ONUs support different security features. Select the security feature recommended in this topic according to actual ONU capabilities.

System Security

Security Vulnerability	Solution	Description and Usage Suggestion
DoS attack	Enable the anti-DoS-attack function for OLT and MDU.	After the anti-DoS-attack function is enabled, control packets are monitored and those exceeding the number threshold are discarded. Use this solution for new site deployment.
IP attack	Enable the anti-IP-attack function for OLT and MDU.	After the anti-IP-attack function is enabled, a device discards the IP packets received from the user side whose destination IP address is the IP address of the device, and therefore the system is protected. Use this solution for new site deployment.

Copyright © Huawei Technologies Co., Ltd.

User Security

Security Vulnerability	Solution	Description and Usage Suggestion
MAC spoofing	Enable the anti-MAC-duplicate function for OLT and MDU.	After anti-MAC-duplicate is enabled, the system records the first MAC address learnt from the port and binds the MAC address to the port and VLAN. If receiving packets sent from the host that has the same MAC address with the port, the system discards the packets directly. In this case, it can prevent users from forging MAC addresses to perform malicious attacks. Use this solution for new site deployment.
MAC attack	Enable the anti-MAC spoofing function for OLT and MDU.	After anti-MAC spoofing is enabled, the system can prevent users from forging IP addresses to perform malicious attacks. Use this solution for new site deployment.
IP spoofing	Enable the anti-IP spoofing function for MDU.	After anti-IP spoofing is enabled, the system can prevent users from forging IP addresses to perform malicious attacks. Use this solution for new site deployment.

14.2.6 Planning Reliability Data

Reliability planning covers planning of equipment reliability and upstream/downstream networking protection. Reliability planning helps to achieve high reliability of private line services.

Copyright © Huawei Technologies Co., Ltd.

Equipment Reliability

Protection Scheme	Description	Suggestion
Main control board 1 +1 protection	The system uses two main control boards of the same model and version. The two main control boards work in the active/standby mode by default. When the active main control board fails, the system switches to the standby main control board to prevent service interruption.	Mandatory
Power board 1+1 protection	A subrack is configured with two power boards of the same model and version, which back up each other. When one of the power board fails, the other power board can still provide power supply to the device and so the system can still work properly.	Mandatory
Upstream board 1+1 protection	The system uses two upstream interface boards of the same model and version. Each GIU board provides one upstream port and two upstream ports are bound together using Link Aggregation Control Protocol (LACP). When the active upstream port fails, traffic will be transmitted upstream through the standby upstream port.	This protection scheme is recommended when the GIU board is used to transmit traffic upstream.

Upstream Networking Protection

Protection Scheme	Description	Suggestion
Link aggregation group	Multiple Ethernet ports are bound together as an aggregation group to increase the bandwidth and balance the inbound and outbound load of each member port. In addition, the ports in an aggregation group back up each other, which enhances the reliability of links.	This protection scheme is mandatory when the GIU board is used to transmit traffic upstream.

Copyright © Huawei Technologies Co., Ltd.

Protection Scheme	Description	Suggestion
Protection group (Ethernet/STM-1)	A protection group of upstream ports contains a working port and a protection port. In normal state, the working port carries services and the protection port does not. When the link at the working port is faulty, the system automatically switches services from the working port to the protection port to ensure normal service transmission and protect the uplink.	When the main control board is used to transmit traffic upstream, this protection scheme is mandatory. This protection scheme is recommended when traffic is transmitted upstream through STM-1 ports.

NOTE

Link aggregation group and Ethernet protection group usually are not configured at the same time. You are advised to configure only one of the two protection schemes.

Downstream Networking Protection

Protection Scheme	Description	Suggestion
xPON Type B	Two PON ports on the same OLT back up each other. When one of the PON ports fails, the system automatically switches to the other PON port. This protection scheme provides port-level protection with low costs. It protects services against fiber failure at the working port.	It rovides port-level protection and has a low cost. The inter-board protection mode is recommended.
GPON Type C single homing	Two PON ports on the same OLT, two PON ports on an ONU, two backbone optical fibers, two optical splitters, and two tributary optical fibers are configured to provide link-level protection.	It rovides link-level protection.

Copyright © Huawei Technologies Co., Ltd.

Protection Scheme	Description	Suggestion
GPON Type C dual homing	Two PON ports on different OLTs, two PON ports on an ONU, two backbone optical fibers, two optical splitters, and two tributary optical fibers are configured to implement this protection. The difference between this protection scheme and the GPON Type C single homing protection scheme is that the ONU needs to be dual homed to two OLTs in this protection scheme. This full-backup protection scheme provides the highest-level protection for links and has the highest costs.	It provides full backup protection, which is the highest level of protection, at the same time, it has the highest cost. This protection scheme can be configured for only the Ethernet QinQ private line service. It does not support TDM services, including Native TDM and SAToP.

NOTE

The Type B protection scheme, Type C single homing scheme, and Type C dual homing protection scheme are mutually exclusive. Therefore, only one of these protection schemes can be configured for an ONU.

14.3 Configuring Base station access Clock Synchronization

This topic describes the concept and principle of clock synchronization in bse station access network, clock synchronization solutions supported by devices, and configuration differences.

14.3.1 Overview of Base station access Clock/Time Synchronization

This topic describes the clock/time synchronization concept, clock/time synchronization solutions supported by the system, and solution comparison. Proper clock synchronization solutions are selected for Base station access networks based on base station type and equipment layout.

Synchronization Concept

Synchronization includes frequency synchronization and time synchronization.

Frequency synchronization is also called clock synchronization, which indicates that certain strict relations are kept between signals in terms of frequency and phase. The valid transience occurs at the same rate for a signal. In this way, the equipment in the entire network runs at the same rate.

Time synchronization is also called frequency and phase synchronization, which has two meanings: instant and interval. Instant refers to an instant of continuous time, and interval refers to an interval between two instants.

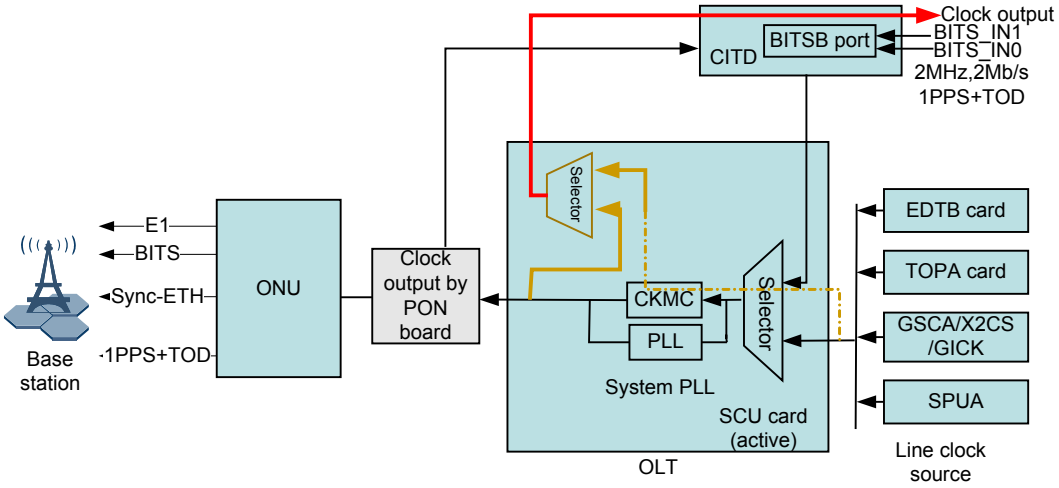
The purpose of clock/time synchronization is to control the occurrence of controlled slip and to decrease the slip, burst bit error, sudden phase change, jitter, or drift of various device signals in the telecommunications service network to the minimum, ensuring the high-quality and high-efficiency running of the telecommunications service network.

Copyright © Huawei Technologies Co., Ltd.

Clock/Time Synchronization Solution

Figure 14-1 shows a clock/time synchronization solution in base station access network. The clock/time synchronization principle is as follows: The clock obtained by the OLT serves as the clock source and transmits signals to the base station through xPON lines.

Figure 14-1 Clock/Time synchronization solution in base station access network



The figure shows that the OLT can obtain the following clock sources:

- BITS clock source
- E1/STM-1/T1 line clock source
- Synchronous Ethernet line clock
- "1PPS+ToD" time injection
- End-to-end 1588v2 clock source
- Internal clock sources are not recommended because they are in free oscillation state and do not have advantages in precision.

Comparison of Clock/Time Synchronization Solution

Table 14-2 shows a clock synchronization solution in base station access network.

Copyright © Huawei Technologies Co., Ltd.

Table 14-2 Comparison of clock/time synchronization solution

Synchronization Solution	Usage Scenario	Advantage	Limitation or Hardware Requirements
BITS clock	Applies to the base station that requires only frequency synchronization, such as GSM/ WCDMA. In addition, the OLT must have BITS clock input resources.	1. Clock precision meets the following requirements: ● G.8262 features when CKMC/ CKMD stratum-3 clock units are configured ● EEC specifications defined in G. 8261 when no stratum-3 clock units are configured 2. No requirements on delay, jitter, or pack loss of a PSN network	1. The OLT must have BITS clock resources. 2. BITS clocks cannot provide independent service clocks for each E1 channel. 3. BITS clocks support only frequency synchronization. Board that support this feature: H801CITD (configured with the H801BITSB daughter board)

Copyright © Huawei Technologies Co., Ltd.

Synchronization Solution	Usage Scenario	Advantage	Limitation or Hardware Requirements
E1/STM-1/T1 line clock	Applies to the BTS that requires only frequency synchronization, such as GSM/ WCDMA. In addition, the OLT can directly connect to an SDH network.	1. Clock precision meets the following requirements: ● G.8262 features when CKMC/ CKMD stratum-3 clock units are configured ● EEC specifications defined in G. 8261 when no stratum-3 clock units are configured 2. E1/STM-1 line clocks are all obtained from physical line clocks and they have the best performance in terms of stability and reliability.	1. In E1/STM-1 upstream transmission, the OLT must be in the same office as SDH equipment. 2. E1/STM-1 line clocks support only frequency synchronization. Boards that support this feature: ● STM-1 line clock: H801TOPA (configured with the H801CSSA daughter board) or H801TOPA (configured with the H801O2CE daughter board). ● E1 line clock: H801TOPA (configured with the H801NH1A daughter board), H801TOPA (configured with the H801EH1A daughter board) or H802EDTB. ● T1 line clock: H802EDTB

Copyright © Huawei Technologies Co., Ltd.

Synchronization Solution	Usage Scenario	Advantage	Limitation or Hardware Requirements
Ethernet clock	Applies to the BTS that requires only frequency synchronization, such as GSM/ WCDMA. In addition, the OLT upstream network has the capability of synchronizing Ethernet clocks.	1. Clock precision meets the following requirements: ● G.8262 features when CKMC/ CKMD stratum-3 clock units are configured ● EEC specifications defined in G. 8261 when no stratum-3 clock units are configured 2. No requirements on delay, jitter, or pack loss of a PSN network	1. Ethernet clocks require that MAN PSN networks have the capability of synchronizing Ethernet clocks. 2. Ethernet clocks support only frequency synchronization. Boards that support this feature: H801X2CS, H801GSCA, H801GICK, H801SPUA, and H801SPUF
"1PPS+ToD" time injection	Applies to the BTS that requires time synchronization, such as CDMA2000/ TD-SCDMA/LTE. When the OLT upstream network does not support 1588V2, this solution is recommended.	1. This solution supports time synchronization and frequency synchronization and provides high-precision time. The clock quality meets G. 813 and G.8262 specifications. 2. This solution does not have requirements on PSN networks.	A BITS server must be at the same place as the OLT.

Copyright © Huawei Technologies Co., Ltd.

Synchronization Solution	Usage Scenario	Advantage	Limitation or Hardware Requirements
End-to-end 1588v2 clock	Applies to the BTS that requires time synchronization, such as CDMA2000/ TD-SCDMA/LTE. When the OLT upstream network supports 1588V2 hop by hop, this solution is recommended.	1. This solution supports time synchronization and frequency synchronization and provides high-precision time. The clock quality meets G. 813 and G.8262 specifications. 2. This solution does not require a 1588V2 server on the OLT.	The upstream network of the OLT should support 1588V2 hop by hop.

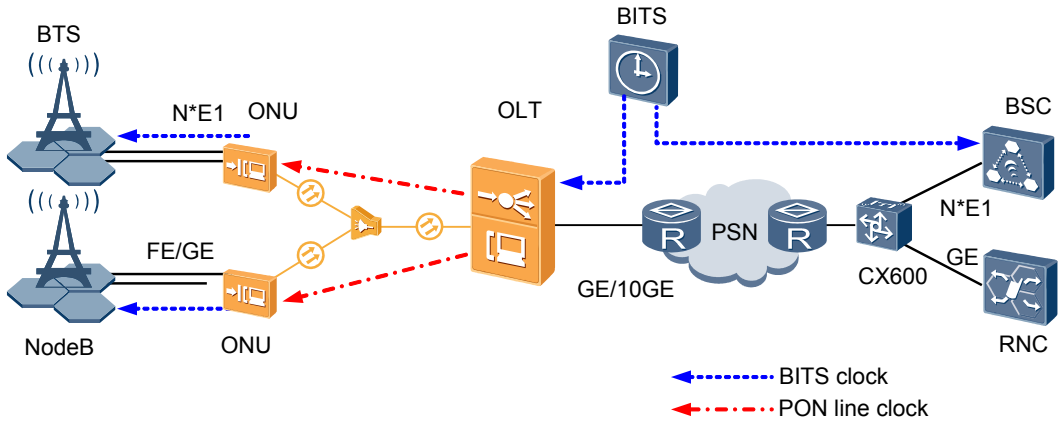
14.3.2 Configuring BITS Clock Synchronization

The OLT receives the clock through the BITS and transmits the clock to the ONU through the PON line and then downstream to the base station, implementing clock synchronization of the entire network.

Application Context

As shown in **Figure 14-2**, the OLT receives the clock from the BITS and the clock share the same clock source with the BSC/RNC. Then the OLT transmits the clock to the ONU through the PON line clock. After recovering the clock, the ONU transmits the clock to the base station through the E1 or FE/GE port.

Figure 14-2 BITS clock synchronization



Copyright © Huawei Technologies Co., Ltd.

Prerequisite

- The clock daughter board CKMC/CKMD of the SCU board must be in position.
- The OLT must have the BITS clock input resource.
- The CITD board (its BITS clock daughter board must be in position) must work in the normal state.

Data Plan

Item	Data
CITD board	Ports: 0/0/0 and 0/0/1 Clock type: BITS 2 MHz, 120 ohms Clock priority: p0 > p1
GIU upstream board	Port: 0/19/0
E1 port of the ONU	0/1/0
ETH port of the ONU	0/4/0

Configuration Concept

1. The OLT uses the BITS line clock as the system clock.
2. The system clock is issued to the ONU through the optical path of the PON service board.
3. The ONU uses the line clock of the PON upstream port as the system clock.
4. The E1 Tx clock of the ONU is synchronized to the system clock of the ONU.

Procedure

Step 1 Configure the OLT-side clock.

1. Configure a system clock source.

   Run the **clock source** command to configure BITS_IN ports 0/0/0 and 0/0/1 on the CITD board as the system clock sources. Set their IDs to 0 and 1 respectively.

   ```
   huawei(config)#clock source 0 0/0/0 2mhz 120ohm
   huawei(config)#clock source 1 0/0/1 2mhz 120ohm
   ```

2. Set the priority of the system clock source.

   Run the **clock priority** command to configure the priorities of clock sources 0 and 1 to p0 > P1.

   ```
   huawei(config)#clock priority system 0/1
   ```

3. Query the configuration and status of the system clock source.

   Run the **display clock source** command to query the configuration and status of the clock source. Ensure that the configuration information about the system clock is matching and the status is normal.

Copyright © Huawei Technologies Co., Ltd.

Step 2 Configure the ONU-side clock.

1. Configure the PON line clock source as the system clock.

   The system clock of the OLT is issued to the ONU through the optical path of the PON port, implementing the clock synchronization between the OLT and the ONU.

   a. Run the **clock source** command to configure the clock recovered from the PON upstream port as the system clock source of the ONU.

   b. Run the **clock priority** command to configure the priority of the clock source.

```
huawei(config)#clock source 0 0/0/1
  Clock source set succeeded

huawei(config)#clock priority system 0
```

2. (Optional) Configure the system clock as the Tx clock of the E1 port.

   NOTE

   This step is required only when the base station is connected to the ONU through the E1 port. When the base station is connected to the ONU through the ETH port, this step is not required. By default, it is the system clock and cannot be modified.

   a. Run the **interface tdm** command to enter the E1 port configuration mode.

   b. Run the **tx clock** or **port** *portid* **udt system** command to configure the Tx clock of the port as the system clock.

   c. Run the **display port state** command to query the Tx clock of the E1 port.

```
huawei(config)#interface tdm 0/1
huawei(config-if-tdm-0/1)#port 0 udt system
huawei(config-if-tdm-0/1)#display port state 0
  ---------------------------------------
  Port           : 0
  State          : normal
  Mode           : UDT
  Code           : HDB3
  Looptype       : -
  Timeslot       : -
  Clock          : system
  CRC4           : -
  Signaling      : -
  ESF            : -
  Impedance      : 120 Ohm
  ---------------------------------------
```

3. Query the configuration and status of the system clock source.

   Run the **display clock source** command to query the configuration and status of the system clock source.

```
huawei(config-if-tdm-0/1)#quit
huawei(config)#display clock source
  ------------------------------------------------------------------------
  Index  Type   Source      State         Priority     QL    Selected
  ------------------------------------------------------------------------
    0    line   0/0/1       Normal          0          ---       YES
    1    --     -/ -/ -     ---             ---        NO        ---
    2    --     -/ -/ -     ---             ---        NO        ---
    3    --     -/ -/ -     ---             ---        NO        ---
    4    --     -/ -/ -     ---             ---        NO        ---
    5    --     -/ -/ -     ---             ---        NO        ---
    6    --     -/ -/ -     ---             ---        NO        ---
    7    --     -/ -/ -     ---             ---        NO        ---
    8    --     -/ -/ -     ---             ---        NO        ---
    9    --     -/ -/ -     ---             ---        NO        ---
  ------------------------------------------------------------------------
```

----End

Copyright © Huawei Technologies Co., Ltd.

Result

After the configuration of base station access service is complete, use the test meter to perform tests on the E1/ETH access port of the ONU and the upstream GE/10GE port. The long-term bit error ratio (BER) and delay should be able to meet the requirements for actual applications.

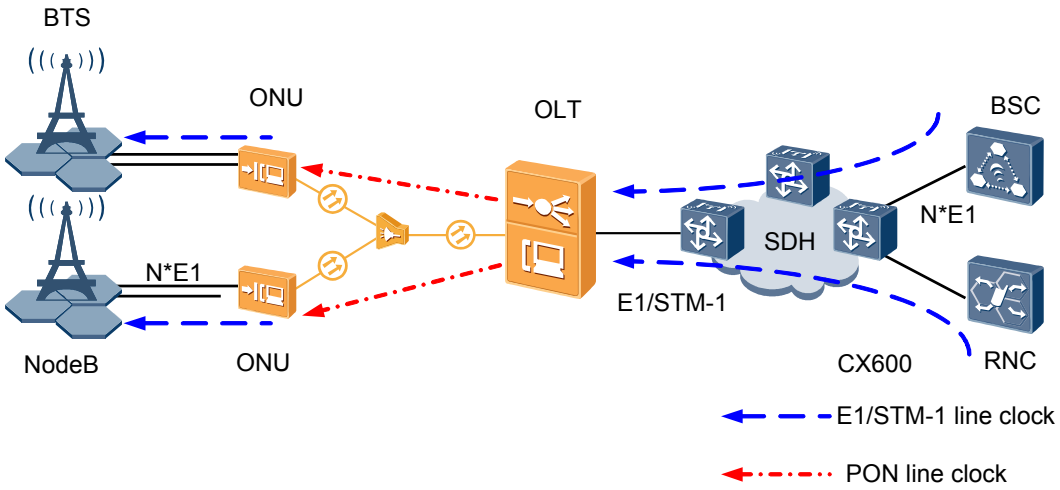
14.3.3 Configuring E1/STM-1 Line Clock Synchronization

When optical line terminals (OLTs) access a base station that requires only frequency synchronization, such as GSM/WCDMA, and when OLTs are connected upstream to the synchronous digital hierarchy (SDH) network by using the E1/STM-1 port, the E1/STM-1 line clock can be used for clock synchronization.

Application Context

As shown in **Figure 14-3**, the OLT recovers the clock from the E1/STM-1 line. This clock is transmitted by the BSC/RNC through the SDH network and then transmitted to the ONU through the PON line clock. After recovering the clock, the ONU transmits the clock to the base station through the E1 line.

Figure 14-3 E1/STM-1 line clock synchronization



Prerequisite

The clock daughter board CKMC/CKMD of the SCU board must be in position.

Copyright © Huawei Technologies Co., Ltd.

Data Plan

Item	Data
TOPA board	Port ID: 0/5/0 Daughter board type: ● When the OLT and the ONU adopt the Native TDM mode, NH1A provides the E1 port and O2CE provides the STM-1 port.
E1 port of the ONU	0/1/0

Configuration Concept

1. The OLT traces the upstream E1/STM-1 line clock of the TOPA board as the system clock.
2. The system clock is issued to the ONU through the optical path of the PON service board.
3. The ONU uses the line clock of the PON upstream port as the system clock.
4. The E1 Tx clock of the ONU is synchronized to the system clock of the ONU.

Procedure

Step 1 Configure the OLT-side clock.

1. Configure a system clock source.

   Run the **clock source** command to configure the line clock of E1/STM-1 port 0/5/0 on the TOPA board as the system clock source. Set the clock source ID to 0.

   The clock module automatically judges the types of the specified clock sources (E1/STM-1) and selects them according to their priority, serving as the clock sources for phase lock.

   ```
   huawei(config)#clock source 0 0/5/0
   ```

2. Set the priority of the system clock source.

   Run the **clock priority** command to configure clock source 0 to have the highest priority.

   ```
   huawei(config)#clock priority system 0
   ```

3. Query the configuration and status of the system clock source.

   Run the **display clock source** command to query the configuration and status of the clock source. Ensure that the configuration information about the system clock is matching and the status is normal.

Step 2 Configure the ONU-side clock.

1. Configure the PON line clock source as the system clock.

   The system clock of the OLT is issued to the ONU through the optical path of the PON port, implementing the clock synchronization between the OLT and the ONU.

   a. Run the **clock source** command to configure the clock recovered from the PON upstream port as the system clock source of the ONU.

   b. Run the **clock priority** command to configure the priority of the clock source.

   ```
   huawei(config)#clock source 0 0/0/1
     Clock source set succeeded
   ```


Copyright © Huawei Technologies Co., Ltd.

```
huawei(config)#clock priority system 0
```

2. Configure the system clock as the Tx clock of the E1 port.
   a. Run the **interface tdm** command to enter the E1 port configuration mode.
   b. Run the **tx clock** or **port** *portid* **udt system** command to configure the Tx clock of the port as the system clock.
   c. Run the **display port state** command to query the Tx clock of the E1 port.

```
huawei(config)#interface tdm 0/1
huawei(config-if-tdm-0/1)#port 0 udt system
huawei(config-if-tdm-0/1)#display port state 0
  ---------------------------------------
  Port          : 0
  State         : normal
  Mode          : UDT
  Code          : HDB3
  Looptype      : -
  Timeslot      : -
  Clock         : system
  CRC4          : -
  Signaling     : -
  ESF           : -
  Impedance     : 120 Ohm
  ---------------------------------------
```

3. Query the configuration and status of the system clock source.

   Run the **display clock source** command to query the configuration and status of the system clock source.

```
huawei(config-if-tdm-0/1)#quit
huawei(config)#display clock source
  ------------------------------------------------------------------------
  Index  Type   Source      State         Priority     QL    Selected
  ------------------------------------------------------------------------
    0    line   0/0/1       Normal          0          ---       YES
    1    --     -/ -/ -     ---             ---        NO        ---
    2    --     -/ -/ -     ---             ---        NO        ---
    3    --     -/ -/ -     ---             ---        NO        ---
    4    --     -/ -/ -     ---             ---        NO        ---
    5    --     -/ -/ -     ---             ---        NO        ---
    6    --     -/ -/ -     ---             ---        NO        ---
    7    --     -/ -/ -     ---             ---        NO        ---
    8    --     -/ -/ -     ---             ---        NO        ---
    9    --     -/ -/ -     ---             ---        NO        ---
  ------------------------------------------------------------------------
```

----End

Result

After the configuration of base station access service is complete, use the test meter to perform tests on the E1 port of the ONU and the upstream E1/STM-1 port of the TOPA board. The long-term bit error ratio (BER) and delay should be able to meet the application requirements.

14.3.4 Configuring Ethernet Clock Synchronization

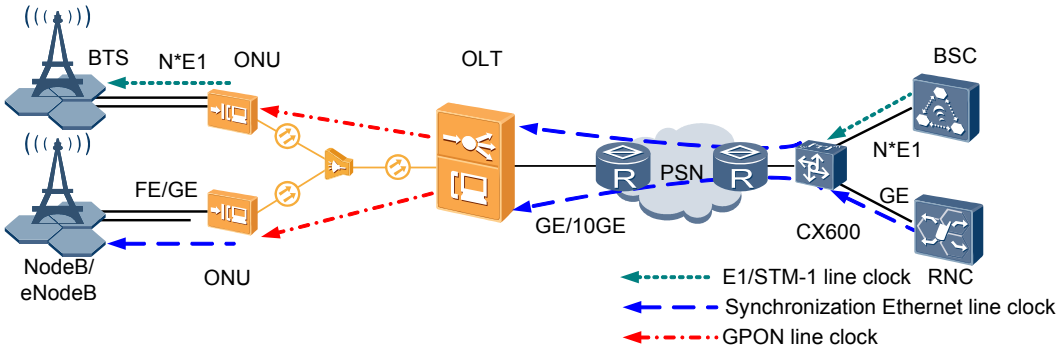
When OLTs access a base transceiver station (BTS) that requires only frequency synchronization, such as GSM/WCDMA/FDD LTE and when the OLTs are connected upstream to the packet switched network (PSN) by using the GE/10GE port, the clock can be recovered from the bit streams on the Ethernet link, implementing synchronization between over the entire network.

Copyright © Huawei Technologies Co., Ltd.

Application Context

As shown in **Figure 14-4**, the OLT receives the clock from the upstream synchronous Ethernet port. (This clock is transmitted through the PSN network and must be supported by all intermediate nodes.) Then the clock is transmitted to the ONU through the PON line clock. After recovering the clock, the ONU transmits the clock to the base station through the synchronous Ethernet or independent clock port.

Figure 14-4 Ethernet clock synchronization



Prerequisite

- The clock daughter board CKMC/CKMD of the SCU board must be in position.
- The ethernet upstream board must be GICK/GSCA (GE port) or X2CS (10GE port)/SPUF (need an independent service board slot).
- The upstream MAN PSN of the OLT must feature the capability of Ethernet synchronization.

Data Plan

Item	Data
GIU Upstream Boards	Port: 0/19/0
E1 port of the ONU	0/1/0
ETH port of the ONU	0/3/1

Configuration Concept

1. The OLT uses the synchronous Ethernet clock of the upstream slot as the system clock.
2. The system clock is issued to the ONU through the optical path of the PON service board.
3. The ONU uses the line clock of the PON upstream port as the system clock.

Copyright © Huawei Technologies Co., Ltd.

4. The Tx clock of the E1 or ETH port on the ONU is synchronized to the system clock of the ONU.

Procedure

Step 1 Configure the OLT-side clock.

1. Configure a system clock source.

   Run the **clock source** command to configure the line clock of the GE/10GE port on the GIU board as the system clock source. Set the clock source ID to 0.

   The clock module automatically judges the types of the specified clock sources (ETH), and selects them according to their priorities, serving as clock sources for phase lock.

   ```
   huawei(config)#clock source 0 0/19/0
   ```

2. Set the priority of the system clock source.

   Run the **clock priority** command to configure clock source 0 to have the highest priority.

   ```
   huawei(config)#clock priority system 0
   ```

3. Query the configuration and status of the system clock source.

   Run the **display clock source** command to query the configuration and status of the clock source. Ensure that the configuration information about the system clock is matching and the status is normal.

Step 2 Configure the ONU-side clock.

1. Configure the PON line clock source as the system clock.

   The system clock of the OLT is issued to the ONU through the optical path of the PON port, implementing the clock synchronization between the OLT and the ONU.

   a. Run the **clock source** command to configure the clock recovered from the PON upstream port as the system clock source of the ONU.

   b. Run the **clock priority** command to configure the priority of the clock source.

   ```
   huawei(config)#clock source 0 0/0/1
     Clock source set succeeded

   huawei(config)#clock priority system 0
   ```

2. (Optional) Configure the system clock as the Tx clock of the E1 port.

   NOTE

   This step is required only when the base station is connected to the ONU through the E1 port. When the base station is connected to the ONU through the ETH port, this step is not required. By default, it is the system clock and cannot be modified.

   a. Run the **interface tdm** command to enter the E1 port configuration mode.

   b. Run the **tx clock** or **port** *portid* **udt system** command to configure the Tx clock of the port as the system clock.

   c. Run the **display port state** command to query the Tx clock of the E1 port.

   ```
   huawei(config)#interface tdm 0/1
   huawei(config-if-tdm-0/1)#port 0 udt system
   huawei(config-if-tdm-0/1)#display port state 0
     ---------------------------------------
     Port          : 0
     State         : normal
     Mode          : UDT
   ```


Copyright © Huawei Technologies Co., Ltd.

```
  Code          : HDB3
  Looptype      : -
  Timeslot      : -
  Clock         : system
  CRC4          : -
  Signaling     : -
  ESF           : -
  Impedance     : 120 Ohm
  ---------------------------------------
```

3. Query the configuration and status of the system clock source.

   Run the **display clock source** command to query the configuration and status of the system clock source.

```
huawei(config-if-tdm-0/1)#quit
huawei(config)#display clock source
  ------------------------------------------------------------------------
  Index  Type   Source      State         Priority     QL    Selected
  ------------------------------------------------------------------------
    0    line   0/0/1       Normal          0          ---      YES
    1    --     -/ -/ -     ---             ---        NO       ---
    2    --     -/ -/ -     ---             ---        NO       ---
    3    --     -/ -/ -     ---             ---        NO       ---
    4    --     -/ -/ -     ---             ---        NO       ---
    5    --     -/ -/ -     ---             ---        NO       ---
    6    --     -/ -/ -     ---             ---        NO       ---
    7    --     -/ -/ -     ---             ---        NO       ---
    8    --     -/ -/ -     ---             ---        NO       ---
    9    --     -/ -/ -     ---             ---        NO       ---
  ------------------------------------------------------------------------
```

----End

Result

After the configuration of base station access service is complete, use the test meter to perform tests on the E1/ETH access port of the ONU and the upstream GE/10GE port. The long-term bit error ratio (BER) and delay should be able to meet the requirements for actual applications.

14.3.5 Configuring "1PPS+ToD" Clock Synchronization

In the base stations that require time synchronization, such as CDMA2000/TD-SCDMA/LTE, the OLT obtaions time by "1PPS+ToD" time injection way. The OLT transmits the clocks to the ONU through GPON lines and then downstream to the base station, implementing clock synchronization of the entire network.

Context

"1PPS+ToD" is a time synchronization technology. The quality of clock transmitted by "1PPS +ToD" meets the stratum 3 clock requirement and the time quality reaches a submicrosecond precision, which solves the time and clock synchronization problems of the user. In addition, using "1PPS+ToD" can better reduce user's investment. Therefore, it is applicable to the base station access services.

Application Context

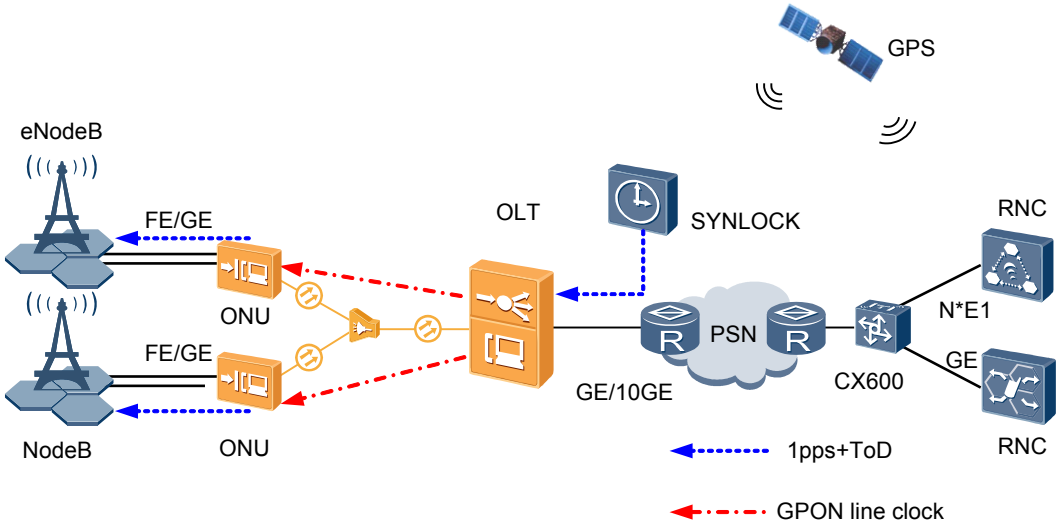
As shown in **Figure 14-5**, the OLT is injected with time through the 1PPS+ToD interface (the time source is obtained from the GPS). Then, the OLT transmits the time signals to the ONU by means of the GPON time synchronization technology. After recovering the time signals, the ONU transmits them to the base station by means of the time interface.

Copyright © Huawei Technologies Co., Ltd.

This scheme has no additional requirement for the PSN network, but the OLT must be deployed with a BITS server (such as SYNLOCK from Huawei). Therefore, this scheme is recommended when the upstream network of the OLT does not support 1588V2.

This scheme requires that ONU supports external clock interface. The model of the ONU supporting this solution is MA5612 and MA5628.

Figure 14-5 "1PPS+ToD" time injection



Prerequisite

- The clock daughter board CKMC/CKMD of the SCU control board must be in position.
- The CITD board (with the BITSB daughter board) must be in position.
- The GPON service board must be GPBD.

Data Plan

Item	Data
Clock source	The time is injected from the BITS IN port of the CITD board to the 1PPS+ToD interface: ● BITS IN ports of the CITD board: 0/0/0 and 0/0/1 ● Clock priority: p0 > p1
ETH port of the ONU	0/3/1

Configuration Concept

1. On the OLT side, select the 1PPS+ToD clock signal as the system clock source.

Copyright © Huawei Technologies Co., Ltd.

2. The system clock is issued to the ONU through the optical path of the PON service board.
3. The ONU uses the 1588V2 clock of the PON upstream port as the system clock.
4. The ONU transmits time signals to the base station by using the FE/GE port or the clock output interface on panel.

Procedure

- **Configure the OLT-side clock.**

  1. Add a "1PPS+ToD" clock source.

     Add two line "1PPS+ToD" clock source, and specify their index and priority.

     ```
     huawei(config)#ptp source 0 0/0/0
     huawei(config)#ptp source 1 0/0/1
     huawei(config)#ptp priority 0/1
     ```

  2. Configure the "1PPS+ToD" clock source as the system clock source.

     ```
     huawei(config)#clock source 0 0/0/0 2mhz 120ohm
     huawei(config)#clock source 1 0/0/0 2mhz 120ohm
     huawei(config)#clock priority system 0/1
     ```

  3. Query the configuration and status of the "1PPS+ToD" clock source and system clock source.

     ```
     huawei(config)#display ptp source
       ------------------------------------------------------------
       Index  Board    Source   State  Priority  Selected  LockState
       ------------------------------------------------------------
         0    H801CITD 0/0/ 0   Normal 0         YES       successful
         1    H801CITD 0/0/ 1   Normal 1                   successful
         2    ---      -/ -/ -  ---    ---       ---       ---
         3    ---      -/ -/ -  ---    ---       ---       ---
         4    ---      -/ -/ -  ---    ---       ---       ---
         5    ---      -/ -/ -  ---    ---       ---       ---
         6    ---      -/ -/ -  ---    ---       ---       ---
         7    ---      -/ -/ -  ---    ---       ---       ---
         8    ---      -/ -/ -  ---    ---       ---       ---
         9    ---      -/ -/ -  ---    ---       ---       ---
       ------------------------------------------------------------
     huawei(config)#display clock source system
       ------------------------------------------------------------------------
       Index  Board    Source   Clk-type  State       Priority QL    Selected
       ------------------------------------------------------------------------
         0    H801CITD 0/0/ 0   2MHz      Normal      0        ---   YES
         1    H801CITD 0/0/ 1   2MHz      Normal      1        ---   ---
       ------------------------------------------------------------------------
     ```

- **Configure the ONU-side clock (the clock is connected to the base station by using GE port to implement time synchronization).**

  This configuration is applicable to time synchronization in the base station where synchronous base station technologies (TDS-CDMA/CDMA2000/LTE is a representative) are adopted. The base station must provide ETH ports and support 1588v2 packets.

  1. Add a system clock source (frequency synchronization).

     The 1588v2 clock is issued to the ONU through the optical path of the PON port, implementing the clock synchronization between the OLT and the ONU.

     a. Run the **clock source** command to add the 1588v2 clock source as the system clock source.

        ```
        huawei(config)#clock source 0 0/0/1
        ```

     b. Run the **clock priority** command to configure the priority of the 1588v2 clock source.

Copyright © Huawei Technologies Co., Ltd.

```
huawei(config)#clock priority system 0
```

2. Configure the 1588v2 time source (time synchronization).

   a. Run the **ptp enable** command to enable the 1588v2 function.
   ```
   huawei(config)#ptp enable
   ```

   b. Run the **ptp source** command to add the 1588v2 clock source as the system clock source.
   ```
   huawei(config)#ptp source 0 0/0/1
   ```

   c. Run the **ptp priority** command to configure the priority of the 1588v2 clock source.
   ```
   huawei(config)#ptp priority 0
   ```

3. Run the **ptp port enable** command to enable the 1588v2 function on the Ethernet port to transmit 1588v2 packets on the specified port.
   ```
   huawei(config)#ptp port 0/3/1 enable
   ```

4. Query the configuration and status of the 1588v2 clock source and system clock source.

   - Run the **display ptp source** command to query the status of the 1588v2 clock source.
   - Run the **display clock source** command to query the configuration and status of the system clock source.

```
huawei(config)#display ptp source
  ------------------------------------------------------------------------
  Index  Type    Source   State     Priority  Selected    Lock state
  ------------------------------------------------------------------------
    0    1588    0/0/1    Normal    0         ---         successful
    1    --      -/ -/ -    ---       ---       ---         ---
    2    --      -/ -/ -    ---       ---       ---         ---
    3    --      -/ -/ -    ---       ---       ---         ---
    4    --      -/ -/ -    ---       ---       ---         ---
    5    --      -/ -/ -    ---       ---       ---         ---
    6    --      -/ -/ -    ---       ---       ---         ---
    7    --      -/ -/ -    ---       ---       ---         ---
    8    --      -/ -/ -    ---       ---       ---         ---
    9    --      -/ -/ -    ---       ---       ---         ---
  ------------------------------------------------------------------------
huawei(config)#display clock source
  ------------------------------------------------------------------------
  Index  Type   Source      State         Priority     QL    Selected
  ------------------------------------------------------------------------
    0    line   0/0/1       Normal          0          ---      YES
    1    --     -/ -/ -     ---             ---        NO       ---
    2    --     -/ -/ -     ---             ---        NO       ---
    3    --     -/ -/ -     ---             ---        NO       ---
    4    --     -/ -/ -     ---             ---        NO       ---
    5    --     -/ -/ -     ---             ---        NO       ---
    6    --     -/ -/ -     ---             ---        NO       ---
    7    --     -/ -/ -     ---             ---        NO       ---
    8    --     -/ -/ -     ---             ---        NO       ---
    9    --     -/ -/ -     ---             ---        NO       ---
  ------------------------------------------------------------------------
```

- **Configure the ONU-side clock (the ONU provides the base station with a clock by using the clock interface on the panel to implement time synchronization).**

  This configuration is applicable to time synchronization in the base station where synchronous base station technologies (TDS-CDMA/CDMA2000/LTE is a representative) are adopted. If a base station provides the ETH port but does not support 1588v2 packets, the ONU outputs 1PPS+ToD time for the base station synchronization.

Copyright © Huawei Technologies Co., Ltd.

1. Add a system clock source (frequency synchronization).

   The 1588v2 clock is issued to the ONU through the optical path of the PON port, implementing the clock synchronization between the OLT and the ONU.

   a. Run the **clock source** command to add the 1588v2 clock source as the system clock source.
   ```
   huawei(config)#clock source 0 0/0/1
   ```
   b. Run the **clock priority** command to configure the priority of the 1588v2 clock source.
   ```
   huawei(config)#clock priority system 0
   ```

2. Configure the 1588v2 time source (time synchronization).

   a. Run the **ptp enable** command to enable the 1588v2 function.
   ```
   huawei(config)#ptp enable
   ```
   b. Run the **ptp source** command to add the 1588v2 clock source as the system clock source.
   ```
   huawei(config)#ptp source 0 0/0/1
   ```
   c. Run the **ptp priority** command to configure the priority of the 1588v2 clock source.
   ```
   huawei(config)#ptp priority 0
   ```

3. Configure the time output mode of the clock output interface.

   The ONU provides an independent output clock through time output port 0 on the panel. Configure the clock output signal to 2 MHz and time signal to 1pps+ubx.

   NOTE

   Configure the clock/time output mode according to actual conditions.

   ```
   huawei(config)#clock bits-type 0 clock 2mhz
     BITS clock parameter set successfully
   huawei(config)#clock bits-type 0 time 1pps protocol ubx
     BITS clock parameter set successfully
   ```

----End

14.3.6 Configuring 1588v2 Clock Synchronization

In the base stations that require time synchronization, such as CDMA2000/TD-SCDMA/LTE, the OLT brings 1588v2 clocks in end-to-end (E2E) 1588v2 mode. The OLT transmits the clocks to the ONU through GPON lines and then downstream to the base station, implementing clock synchronization of the entire network.

Context

1588v2 is a time synchronization technology. The quality of clock transmitted by 1588v2 meets the stratum 3 clock requirement and the time quality reaches a submicrosecond precision, which solves the time and clock synchronization problems of the user. In addition, using 1588v2 can better reduce user's investment. Therefore, 1588v2 is applicable to the base station access services.

Application Context

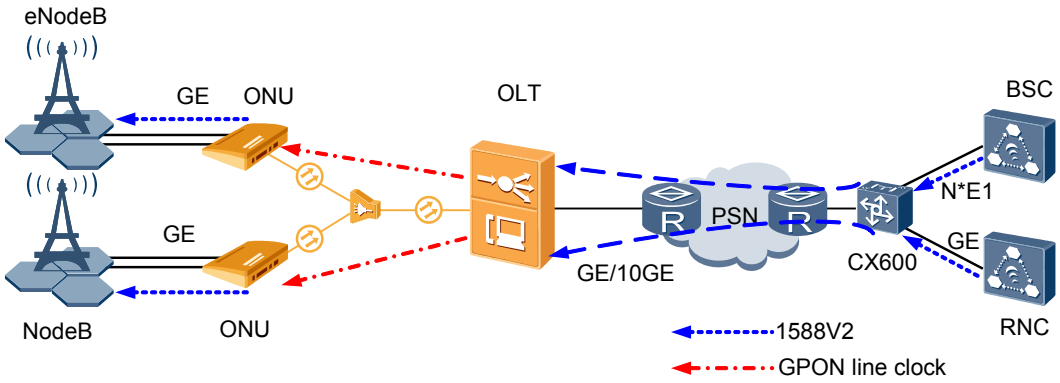
As shown in **Figure 14-6**, the OLT obtains the 1588v2 time by using the upstream network interface (the time is transmitted by the upstream network hop by hop). Then, the OLT transmits

Copyright © Huawei Technologies Co., Ltd.

the time to the ONU through the GPON line. After recovering the time, the ONU transmits the time to the base station by means of the 1588v2 or time interface.

This scheme does not require a 1588v2 server on the OLT. Therefore, this scheme is recommended when the upstream network of the OLT supports 1588v2 hop by hop.

Figure 14-6 E2E 1588v2



Prerequisite

- The clock daughter board CKMC/CKMD of the SCU control board must be in position.
- The GE 1588v2 upstream board GICK or SPUF (10GE) must be in position.
- The GPON service board must be H805GPBD/H806GPBH/H802GPFD.

Data Plan

Item	Data
1588v2 clock source	When the 1588v2 clock packets are injected by using the GICK/SPUF board or the 1588v2 clock packets of the upstream network are transparently transmitted: ● GE ports of the GICK board: 0/19/0 and 0/19/1 ● 10 GE ports of the SPUF board: 0/2/0 and0/2/1 ● Clock source selection mode: priority ● Clock priority: p0 > p1
GPON port	0/3/1
ETH port of the ONU	0/3/1

Copyright © Huawei Technologies Co., Ltd.

Configuration Concept

1. On the OLT side, select the clock signal recovered from 1588v2 packets as the system clock source.
2. The system clock is issued to the ONU through the optical path of the PON service board.
3. The ONU uses the 1588v2 clock of the PON upstream port as the system clock.
4. The Tx clock of the GE port on the ONU is synchronized to the system clock of the ONU.
5. The ONU synchronizes the clock and time with the base station in the following three modes:
   - The ONU transmits 1588v2 packets to the base station by using the GE port.
   - The ONU provides independent time signals to the base station by using the clock output interface.

Procedure

- **Configure the OLT-side clock.**
  1. Configure the global 1588v2 function.

     Run the **ptp enable** command to enable 1588v2 on a device.

     ```
     huawei(config)#ptp enable
     ```

     (Optional) Run the **ptp domain** command to configure a 1588v2 time domain.

     Each time domain supports only one clock source. All the devices in the 1588v2 time domain are synchronized with the clock source. Ensure that the time domain of an MDU is the same as that of the optical line terminal (OLT).

     ```
     huawei(config)#ptp domain 1
     ```

  2. Configure the system clock source and time synchronization (frequency synchronization).
     a. Run the command to configure the index of the system clock source.

        The clock source can be the synchronous clock recovered from a GE or 10 GE line on the network side, 1588v2 clock, or BITS clock.

        When the network supports synchronous Ethernet clock, the clock is recommended.

     b. Run the **clock priority system** command to set the priority of the clock source. A device may trace multiple clock sources for synchronizing the clock. It selects the clock source with the highest priority as the clock source.

     c. **Optional:** Configure the mode for dynamically selecting the system clock source.

        The system supports static and dynamic selection. When dynamic selection is required based on Synchronization Status Message (SSM), run the **clock ql-mode enable** command to enable the SSM selection mode.

     - If the GICK board is used to access the 1588v2 clock source:

       ```
       huawei(config)#clock source 0 0/19/0
       huawei(config)#clock source 1 0/19/1
       huawei(config)#clock priority system 0/1
       ```

     - If the SPUF board is used to access the 1588v2 clock source:

Copyright © Huawei Technologies Co., Ltd.

```
huawei(config)#clock source 0 0/2/0
huawei(config)#clock source 1 0/2/1
huawei(config)#clock priority system 0/1
```

3. Configure a 1588v2 time source (time synchronization).
   a. Run the **ptp source** command to configure a 1588v2 time source.
   b. Configure the mode of selecting the 1588v2 time source.

      A time source can be statically or dynamically selected.

      - To statically select a time source based on the local priority, run the **ptp priority** command to set the priority of the time source.
      - To dynamically select a time source based on the best master clock (BMC), run the **ptp bmc enable** command to configure the status of the automatic BMC source selection function.

   c. Run the **ptp port enable** command to enable 1588v2 on an Ethernet port to transmit 1588v2 packets.

      Enable 1588v2 on the ports that are required to transmit 1588v2 packets, for example, the uplink port on an OLT and user-side port on an MDU. You are not required to enable the function on the GPON port connecting the OLT and MUD.

   - If the GICK board is used to access the 1588V2 clock source:

```
huawei(config)#ptp source 0 0/19/0
huawei(config)#ptp source 1 0/19/1
huawei(config)#ptp priority 0/1
huawei(config)#ptp port 0/19/0 enable
huawei(config)#ptp port 0/19/1 enable
```

   - If the SPUF board is used to access the 1588V2 clock source:

```
huawei(config)#ptp source 0 0/2/0
huawei(config)#ptp source 1 0/2/1
huawei(config)#ptp priority 0/1
huawei(config)#ptp port 0/2/0 enable
huawei(config)#ptp port 0/2/1 enable
```

4. (Optional) Configure the attributes of the 1588 V2 clock source.

   Configure 1588v2 parameters, such as timestamp mode of the 1588v2 packets, MAC encapsulation mode, and UDP encapsulation mode. By default, the MAC mode is used as the packet encapsulation mode, and the L2 multicast mode is used as the packet forwarding mode.

   When the default attributes of the 1588v2 clock source do not meet the actual requirement, run the command to modify the attributes.

   NOTE

   Before modification, ensure that the attributes of the 1588v2 clock source are the same as the actual ones. In this example, assume that the default attributes of the system clock source meet the application requirements.

5. Query the configuration and status of the 1588v2 clock source and system clock source.
   - Run the command to query the status of the 1588v2 clock source.
   - Run the command to query the configuration and status of the system clock source.

```
huawei(config)#display ptp source
  ------------------------------------------------------------------
  Index  Board    Source   State  Priority  Selected   LockState
  ------------------------------------------------------------------
    0    H801GICK 0/19/ 0  Normal 0         YES        successful
    1    H801GICK 0/19/ 1  Normal 1                    successful
```


Copyright © Huawei Technologies Co., Ltd.

```
  2    ---      -/ -/ -  ---    ---       ---      ---
  3    ---      -/ -/ -  ---    ---       ---      ---
  4    ---      -/ -/ -  ---    ---       ---      ---
  5    ---      -/ -/ -  ---    ---       ---      ---
  6    ---      -/ -/ -  ---    ---       ---      ---
  7    ---      -/ -/ -  ---    ---       ---      ---
  8    ---      -/ -/ -  ---    ---       ---      ---
  9    ---      -/ -/ -  ---    ---       ---      ---
 ------------------------------------------------------------------
huawei(config)#display clock source system
 ------------------------------------------------------------------------
 Index  Board    Source   Clk-type  State       Priority QL    Selected
 ------------------------------------------------------------------------
   0    H801GICK 0/19/ 0  ---       Normal      0        ---   YES
   1    H801GICK 0/19/ 1  ---       Normal      1        ---   ---
 ------------------------------------------------------------------------
```

- **Configure the ONU-side clock (the clock is connected to the base station by using GE port to implement time synchronization).**

  This configuration is applicable to time synchronization in the base station where synchronous base station technologies (TDS-CDMA/CDMA2000/LTE is a representative) are adopted. The base station must provide ETH ports and support 1588v2 packets.

  1. Add a system clock source (frequency synchronization).

     The 1588v2 clock is issued to the ONU through the optical path of the PON port, implementing the clock synchronization between the OLT and the ONU.

     a. Run the **clock source** command to add the 1588v2 clock source as the system clock source.
     ```
     huawei(config)#clock source 0 0/0/1
     ```
     b. Run the **clock priority** command to configure the priority of the 1588v2 clock source.
     ```
     huawei(config)#clock priority system 0
     ```

  2. Configure the 1588v2 time source (time synchronization).

     a. Run the **ptp enable** command to enable the 1588v2 function.
     ```
     huawei(config)#ptp enable
     ```
     b. Run the **ptp source** command to add the 1588v2 clock source as the system clock source.
     ```
     huawei(config)#ptp source 0 0/0/1
     ```
     c. Run the **ptp priority** command to configure the priority of the 1588v2 clock source.
     ```
     huawei(config)#ptp priority 0
     ```

  3. Run the **ptp port enable** command to enable the 1588v2 function on the Ethernet port to transmit 1588v2 packets on the specified port.
     ```
     huawei(config)#ptp port 0/3/1 enable
     ```

  4. Query the configuration and status of the 1588v2 clock source and system clock source.

     - Run the **display ptp source** command to query the status of the 1588v2 clock source.
     - Run the **display clock source** command to query the configuration and status of the system clock source.

     ```
     huawei(config)#display ptp source
      ------------------------------------------------------------------
      Index  Type    Source   State     Priority  Selected    Lock state
      ------------------------------------------------------------------
        0    1588    0/0/1    Normal    0         ---         successful
     ```


Copyright © Huawei Technologies Co., Ltd.

```
  1    --     -/ -/ -    ---       ---       ---       ---
  2    --     -/ -/ -    ---       ---       ---       ---
  3    --     -/ -/ -    ---       ---       ---       ---
  4    --     -/ -/ -    ---       ---       ---       ---
  5    --     -/ -/ -    ---       ---       ---       ---
  6    --     -/ -/ -    ---       ---       ---       ---
  7    --     -/ -/ -    ---       ---       ---       ---
  8    --     -/ -/ -    ---       ---       ---       ---
  9    --     -/ -/ -    ---       ---       ---       ---
 ------------------------------------------------------------------------
huawei(config)#display clock source
 ------------------------------------------------------------------------
 Index  Type   Source      State         Priority     QL    Selected
 ------------------------------------------------------------------------
  0    line   0/0/1       Normal          0          ---      YES
  1    --     -/ -/ -     ---             ---        NO       ---
  2    --     -/ -/ -     ---             ---        NO       ---
  3    --     -/ -/ -     ---             ---        NO       ---
  4    --     -/ -/ -     ---             ---        NO       ---
  5    --     -/ -/ -     ---             ---        NO       ---
  6    --     -/ -/ -     ---             ---        NO       ---
  7    --     -/ -/ -     ---             ---        NO       ---
  8    --     -/ -/ -     ---             ---        NO       ---
  9    --     -/ -/ -     ---             ---        NO       ---
 ------------------------------------------------------------------------
```

- **Configure the ONU-side clock (the ONU provides the base station with a clock by using the clock interface on the panel to implement time synchronization).**

  This configuration is applicable to time synchronization in the base station where synchronous base station technologies (TDS-CDMA/CDMA2000/LTE is a representative) are adopted. If a base station provides the ETH port but does not support 1588v2 packets, the ONU outputs 1PPS+ToD time for the base station synchronization.

  1. Add a system clock source (frequency synchronization).

     The 1588v2 clock is issued to the ONU through the optical path of the PON port, implementing the clock synchronization between the OLT and the ONU.

     a. Run the **clock source** command to add the 1588v2 clock source as the system clock source.
     ```
     huawei(config)#clock source 0 0/0/1
     ```
     b. Run the **clock priority** command to configure the priority of the 1588v2 clock source.
     ```
     huawei(config)#clock priority system 0
     ```

  2. Configure the 1588v2 time source (time synchronization).

     a. Run the **ptp enable** command to enable the 1588v2 function.
     ```
     huawei(config)#ptp enable
     ```
     b. Run the **ptp source** command to add the 1588v2 clock source as the system clock source.
     ```
     huawei(config)#ptp source 0 0/0/1
     ```
     c. Run the **ptp priority** command to configure the priority of the 1588v2 clock source.
     ```
     huawei(config)#ptp priority 0
     ```

  3. Configure the time output mode of the clock output interface.

     The ONU provides an independent output clock through time output port 0 on the panel. Configure the clock output signal to 2 MHz and time signal to 1pps+ubx.

     NOTE

     Configure the clock/time output mode according to actual conditions.

Copyright © Huawei Technologies Co., Ltd.

```
huawei(config)#clock bits-type 0 clock 2mhz
  BITS clock parameter set successfully
huawei(config)#clock bits-type 0 time 1pps protocol ubx
  BITS clock parameter set successfully
```

----End

Result

After the FTTM service configuration is complete, use the test meter to perform tests on the ETH access port of the ONU and the upstream GE/10GE port of the OLT. The long-term bit error ratio (BER) and delay should be able to meet the requirements for actual applications.

14.4 Configuring Base Station Access Service (GPON)

This topic describes how to configure the base station access service in GPON mode in different networking scenarios.

Context

There are two xPON configuration modes: distributed mode (also called discrete mode) and profile mode. The difference between the two modes lies in command lines.

- Distributed mode: In this mode, ONTs need to be configured one by one but not in batches.
- Profile mode: In this mode, an ONT line profile and service profile are configured first. Then, ONTs can be added in batches by binding profiles. This mode greatly improves service provisioning efficiency.

Generally, the xPON configuration mode is determined in a new deployment and will not be changed. This chapter describes how to configure the enterprise access service in PON profile mode (which is the default mode). You can run the commands in the following table to query the xPON configuration mode.

Mode	Query Method
PON profile mode	huawei(config)#**diagnose** huawei(diagnose)%%**display xpon mode** --- Current config mode: Profile-mode ---

NOTE

For commands for the distributed configuration mode, see **PON distributed-mode commands** in the *Command Reference*.

14.4.1 E1 Base Station Access Service (in Native TDM Mode)

ONUs transmit E1 signals of base stations to OLTs in Native TDM mode and OLTs are interconnected with transmission equipment through E1/STM-1 ports. In this manner, traditional circuit switching services can be carried over GPON networks.

14.4.1.1 Service Requirement and Application Scenario

Copyright © Huawei Technologies Co., Ltd.

Service Requirement

As a mainstream full-service access technology in the future, the passive optical network (PON) supports fast deployment and service provisioning. It also helps simplify the access network and reduce the costs on construction and subsequent maintenance of the access network. Currently, carriers in China and outside China are using the PON to carry 2G/3G base station services over their existing FTTx networks that are established for accessing individual/enterprise users. In this manner, carriers can implement the access of all the services at the access layer in an unified mode.

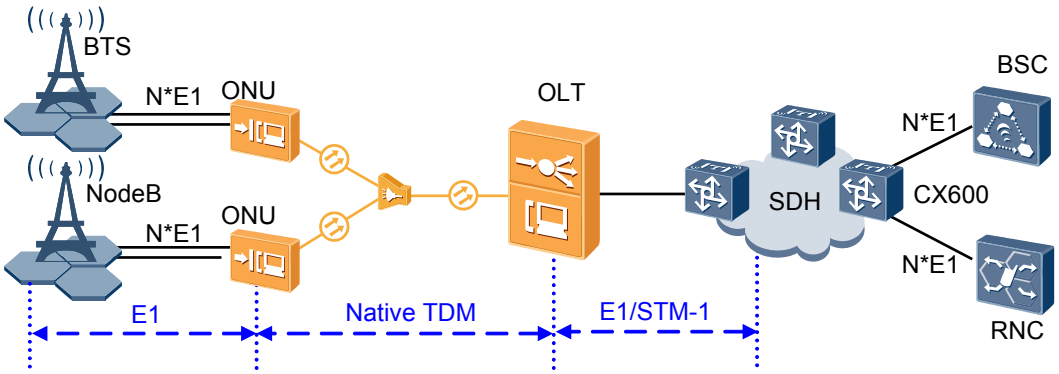
- ONUs are connected to 2G or 3G base stations through E1 ports.
- GPON is used for carrying the mobile access network in a unified manner to meet mobile carriers' requirements for a high bandwidth and high-density coverage of base stations.
- Existing SDH resources are utilized efficiently to implement high-quality transmission of TDM services.

Application Scenario

As shown in **Figure 14-7**, the ONU accesses TDM services of the 2G or 3G base station through the E1 port, and then transmits the service data to the GPON service board on the OLT in the Native TDM mode. The OLT restores TDM signals, and then transmits the signals to the SDH network through the E1 port (provided by the NH1A daughter board) or STM-1 port (provided by the O2CE daughter board) on the TOPA board. In this manner, service access of the 2G or 3G base station is implemented between the ONU and the OLT in the Native TDM mode.

Applicable ONUs: MA5612, MA5628, MA5616

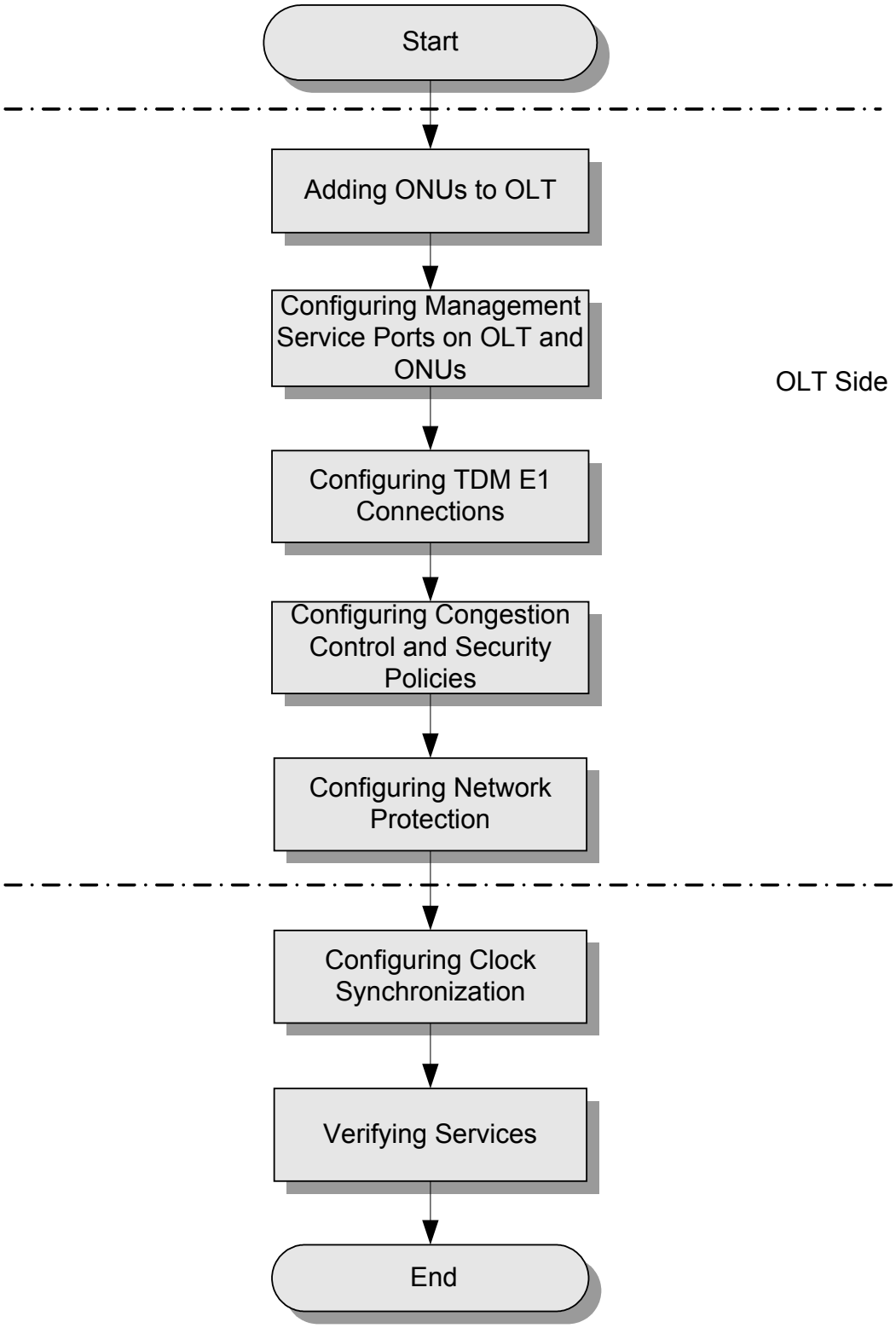
Figure 14-7 Networking diagram of E1 base station access service



14.4.1.2 Configuration Process

The following figure shows the configuration process for E1 base station access service.

Copyright © Huawei Technologies Co., Ltd.



14.4.1.3 Adding ONUs to OLT

This topic describes how to add ONUs to the OLT. ONUs can be configured only after they are added to the OLT successfully.

Copyright © Huawei Technologies Co., Ltd.

Context

- When adding ONUs, you need to bind related profiles to the ONUs, including the DBA profile, line profile, and alarm profile.
- An ONU can be added in two modes: offline addition and online confirmation. Select either mode as required.

Data Plan

Table 14-3 Key data plan

Configuration Item	Data
DBA profile	DBA profile for management service: dba-profile_1 (system default) DBA profile for private line service: ● Profile ID: 21 ● Profile type: Fixed bandwidth and minimum delay ● DBA bandwidth: 28928 kbit/s (Each ONU accesses four E1 private lines and each line has a recommended DBA bandwidth of 7232 kbit/s.)
Line profile	Profile ID: 11 T-CONT ID: 1 (for private line service) and 2 (for management service) GEM port ID for management service: 11 GEM port ID for DDN private line service: 13
Networking data	PON port: 0/3/1 ONU parameters: ● ONU ID: 1 ● SN: 32303131B39FD641

Procedure

Step 1 Configure GPON ONU profiles.

1. Configure a DBA profile. Enable the bandwidth compensation function and set the DBA bandwidth allocation mode for the GPON port to minimum bandwidth delay.

```
huawei(config)#dba-profile add profile-id 21 type1 fix 28928
bandwidth_compensate yes
huawei(config)#interface gpon 0/3
huawei(config-if-gpon-0/3)#port dba bandwidth-assignment-mode 1 min-loop-delay
huawei(config-if-gpon-0/3)#quit
```

2. Configure an ONU line profile.

```
huawei(config)#ont-lineprofile gpon profile-id 11
huawei(config-gpon-lineprofile-11)#tcont 1 dba-profile-id 21  //Bind T-CONT 1
to DBA profile 21
huawei(config-gpon-lineprofile-11)#tcont 2 dba-profile-id 1  //Bind T-CONT 2
to DBA profile 1
huawei(config-gpon-lineprofile-11)#gem add 11 eth tcont 2
huawei(config-gpon-lineprofile-11)#gem add 13 tdm tcont 1 //Add GEM port 13 to
```


Copyright © Huawei Technologies Co., Ltd.

```
T-CONT 1.
huawei(config-gpon-lineprofile-11)#gem mapping 11 0 vlan 8
huawei(config-gpon-lineprofile-11)#gem mapping 13 1 e1 1 //Map GEM port 13 to
E1 port 1 on the ONU.
huawei(config-gpon-lineprofile-11)#commit
huawei(config-gpon-lineprofile-11)#quit
```

3. (Optional) Configure an alarm profile.
   - The default GPON alarm profile ID is 1. The value of each alarm threshold is **0** which indicates that alarms are not reported.
   - In this example, the default alarm profile is used and no configuration is required.

Step 2 Add ONUs to the OLT.

1. Add ONU 3 in offline mode.

```
huawei(config)#interface gpon 0/3
huawei(config-if-gpon-0/3)#ont add 1 ontid 1 sn-auth 32303131B39FD641
snmp ont-lineprofile-id 11
```

2. (Optional) Bind an alarm profile.

   By default, an ONU will be automatically bound to alarm profile 1 (default profile). You need to manually bind an alarm profile to an ONU only when the default alarm profile does not meet requirements.

   In this example, the default alarm profile is used. Therefore, you do not need to manually bind an alarm profile.

Step 3 Confirm the ONU status.

After adding an ONU, run the **display ont info** command to query the current status of the ONU. Ensure that **Control flag** is **active**, **Run State** is **online**, and **Config state** is **normal**.

The following uses ONU 1 as an example to describe how to confirm ONU status.

```
huawei(config-if-gpon-0/3)#display ont info 1 1
  ------------------------------------------------------------------------
  F/S/P                : 0/3/1
  ONT-ID               : 1
  Control flag         : active    //Indicates that the ONU is
activated.
  Run state            : online    //Indicates that the ONU is
online.
  Config state         : normal    //Indicates that the ONU is in normal
state.
...//Other command output is omitted.
huawei(config-if-gpon-0/3)#quit
```

----End

Follow-up Procedure

When **Config state** is **failed**, **Run state** is **offline**, or **Match state** is **mismatch**:

- If **Control flag** is **deactive**, run the **ont active** command in GPON mode to activate the ONU.
- If **Run state** is **offline**, a physical line may be broken or the optical module may be damaged. Check the line and the optical module.
- If **Config state** is **failed**, the configured ONU capability exceeds the actual ONU capability. In this case, run the **display ont failed-configuration** command in the diagnose mode to check the failed configuration item and the failure cause. Then, rectify the fault accordingly.

Copyright © Huawei Technologies Co., Ltd.

- If the ONU does not match, that is, **Match state** is **mismatch**, the port types and number of ports undermatch the actual port types and number of ports supported by the ONU. In this case, run the **display ont capability** command to query the actual capability of the ONU, and then select one of the following modes to modify the ONU configuration:
  - Create a proper ONU profile according to the actual capability of the ONU, and then run the **ont modify** command to modify the configuration data of the ONU.
  - Modify the ONU profile according to the actual capability of the ONU and save the modification. Then, the ONU automatically recovers the configuration successfully.

14.4.1.4 Configuring Management Service Ports on OLT and ONUs

This topic describes how to configure management service ports (also called service flows) on the OLT and ONUs. After the connections between the in-band management service ports on the OLT and ONUs are reachable, you can log in to the ONUs on the OLT and configure the ONUs.

Data Plan

Configuration Item	Data
Management VLAN and management IP address for OLT	Management VLAN ID: 8 Management VLAN type: smart In-band management IP address: 192.168.50.1/24
Management VLAN and management IP address for ONU	Management VLAN ID: 8 Management VLAN type: smart In-band management IP address for ONU 3: 192.168.50.2/24

Procedure

Step 1 Configure the in-band management VLAN and IP address for the OLT.

Set the in-band management VLAN to 8, VLAN priority to 6, and IP address to 192.168.50.1/24.

```
huawei(config)#vlan 8 smart
huawei(config)#port vlan 8 0/19 0
huawei(config)#vlan priority 8 6
huawei(config)#interface vlanif 8
huawei(config-if-vlanif8)#ip address 192.168.50.1 24
huawei(config-if-vlanif8)#quit
```

Step 2 Configure the in-band management VLAN and IP address for the ONU.

```
huawei(config)#interface gpon 0/3
huawei(config-if-gpon-0/3)#ont ipconfig 1 1 static ip-address 192.168.50.2 mask
255.255.255.0 gateway
192.168.50.1 vlan 8
huawei(config-if-gpon-0/3)#quit
```

Step 3 Configure the in-band management service port.

Copyright © Huawei Technologies Co., Ltd.

Set the management VLAN to 8, GEM port ID to 11, and user VLAN to 8. The OLT does not rate limit the in-band management service port. Therefore, directly use the default traffic profile 6.

```
huawei(config)#service-port vlan 8 gpon 0/3/1 ont 1 gemport 11 multi-service
user-vlan 8 rx-cttr 6 tx-cttr 6
```

Step 4 Confirm that the connection between the management service ports on the OLT and ONU is reachable.

- Run the **ping *ONU ip*** command on the OLT to verify the connectivity between the OLT and ONU. If the OLT receives ICMP ECHO-REPLY packets from the ONU, the connection is reachable.
- When the connection is reachable, you can remote log in to the ONU from the OLT and configure the ONU.

----End

14.4.1.5 Configuring TDM E1 Connections

This topic describes how to configure Native TDM connections between GPON ports and E1/STM-1 upstream ports to transmit E1/STM-1 private line service data.

Prerequisites

Required hardware is available:

- TOPA+NH1A for upstream transmission through E1
- TOPA+O2CE for upstream transmission through STM-1
- GPON board: GPBC, GPBD

Context

The OLT can transmit data to the SDH network through E1 or STM-1 lines. Each E1 line provides 2 Mbit/s bandwidth. After being mapped, aligned, and encapsulated, 63xE1 signals are multiplexed into one STM-1 signal through VC12. One STM-1 line provides 155 Mbit/s.

When the OLT transmits data to SDH equipment through STM-1 lines, pay attention to the VC12 mode and VC12 number.

- When the OLT is interconnected with Huawei SDH equipment, the VC12 mode is huawei and the VC12 numbers on the OLT and the SDH equipment must be consistent.
- When the OLT is interconnected with Lucent SDH equipment, the VC12 mode is lucent. The VC12 numbers has the following mapping relationships (which can be queried using the **display vc12-mode-table** command):

  Huawei: Mapping between the multiplexing number and VC12 number: VC12 number = (TUG3–1) + (TUG2–1) x 3 + (TU12–1) x 21

  Lucent: Mapping between the multiplexing number and VC12 number: VC12 number = (TU12–1) + (TUG2–1) x 3 + (TUG3–1) x 21

Copyright © Huawei Technologies Co., Ltd.

Data Plan

Upstream Transmission Mode	Data
Upstream transmission through E1	Port on the TOPA board: 0/5/0 Daughter board type: NH1A (provides E1 ports)
Upstream transmission through STM-1	Port on the TOPA board: 0/5/0 Daughter board type: O2CE (provides STM-1 ports) VC12 number: 0 **NOTE** The VC12 parameter must match that on the interconnected SDH equipment. Otherwise, services fail.

Procedure

- Configure a TDM E1 connection for E1 upstream transmission.

  ```
  huawei(config)#tdm-connect connectid 1 tdm 0/5/0 gpon 0/3/1 ontid 3 gemportIndex 13
  ```

- Configure a TDM E1 connection for STM-1 upstream transmission.

  ```
  huawei(config)#tdm-connect connectid 1 tdm 0/5/0 vc12 0 gpon 0/3/1 ontid 3 gemportIndex 13
  ```

----End

14.4.1.6 Configuring Clock Synchronization

In this scenario, the E1/STM-1 line clock can be used to achieve network-wide clock synchronization.

Prerequisites

The clock daughter board CKMC/CKMD must be on the SCU main control board.

Context

Configuration roadmap for clock synchronization:

1. The OLT traces the upstream E1/STM-1 line clock of the TOPA board as the system clock.
2. The system clock is delivered to an ONU through optical paths of the GPON board.
3. The ONU uses the line clock of the GPON upstream port as the system clock.
4. The ONU E1 transmit clock is synchronized with the system clock of the ONU.

Procedure

- **Configure a clock on the OLT.**
  1. Add a system clock source.

Copyright © Huawei Technologies Co., Ltd.

Run the **clock source** command to configure the line clock of E1/STM-1 port 0/5/0 on the TOPA board as the system clock source. Set the ID of the clock source to 0.

The clock module automatically judges the type of the specified clock source (E1/STM-1) and selects a reference source for phase lock based on priorities.

```
huawei(config)#clock source 0 0/5/0
```

2. Configure a priority for the system clock source.

   Run the **clock priority** command to set the priority of clock source 0 to the highest priority.

```
huawei(config)#clock priority system 0
```

3. Query configurations and the status of the system clock source.

   Run the **display clock source system** command to query configurations and the status of the clock source. Ensure that configurations of the system clock source are correct and the status is **Normal**.

```
huawei(config)#display clock source system

-------------------------------------------------------------------------
-----
  Index  Board    Source   Clk-type  State       Priority QL
Selected

-------------------------------------------------------------------------
-----
    0    H801TOPA 0/5/0    E1        Normal      0        ---
YES

-------------------------------------------------------------------------
-----
```

   Run the **display clock mode** command to query the clock working mode. Ensure that the clock daughter board works in tracing mode.

```
huawei(config)#display clock mode
  Clock manage-mode:Third-mode
  Clock subboard work-mode:Tracing
```

- **Configure a clock on the ONU.**

1. Configure the GPON line clock as the system clock.

   The system clock of the OLT is delivered to the ONU through the GPON port on the OLT, achieving clock synchronization between the OLT and the ONU.

   a. Run the **clock source** command to configure the clock recovered from the GPON upstream port as the system clock of the ONU.

   b. Run the **clock priority** command to configure the priority of the clock source.

```
huawei(config)#clock source 0 0/0/1
  Clock source set succeeded

huawei(config)#clock priority system 0
```

2. Configure the system clock as the transmit clock for an E1 port.

   a. Run the **interface tdm** command to enter the E1 port configuration mode.

   b. Run the **tx clock** or **port** *portid* **udt system** command to configure the system clock as the transmit clock of the port.

   c. Run the **display port state** command to query the transmit clock of the E1 port.

```
huawei(config)#interface tdm
huawei(config-if-tdm-)#port 0 udt system
```


Copyright © Huawei Technologies Co., Ltd.

```
huawei(config-if-tdm-)#display port state 0
  ---------------------------------------
  Port           : 0
  State          : normal
  Mode           : UDT
  Code           : HDB3
  Looptype       : -
  Timeslot       : -
  Clock          : system
  CRC4           : -
  Signaling      : -
  ESF            : -
  Impedance      : 120 Ohm
  ---------------------------------------
```

3. Query configurations and the status of the system clock source.

   Run the **display clock source** command to query configurations and the status of the system clock source.

```
huawei(config-if-tdm-)#quit
huawei(config)#display clock source
  ------------------------------------------------------------------
  Index  Config   Type   Source      State     Priority   Output
  ------------------------------------------------------------------
    0    YES      line   0/0/1       Normal    0          YES
    1    NO       --     -/ -/ -     ---       ---        ---
    2    NO       --     -/ -/ -     ---       ---        ---
    3    NO       --     -/ -/ -     ---       ---        ---
    4    NO       --     -/ -/ -     ---       ---        ---
    5    NO       --     -/ -/ -     ---       ---        ---
    6    NO       --     -/ -/ -     ---       ---        ---
    7    NO       --     -/ -/ -     ---       ---        ---
    8    NO       --     -/ -/ -     ---       ---        ---
    9    NO       --     -/ -/ -     ---       ---        ---
  ------------------------------------------------------------------
```

----End

14.4.1.7 Configuring Congestion Control and Security Policies

This topic describes how to configure global priority-based scheduling policies for queues to ensure service reliability and configure global security policies to ensure service security.

Context

Congestion control uses queue scheduling technology to map packets sent from the same port into multiple queues and process packets in each queue based on priority. Congestion control is recommended.

Security policies cover system security, user security, and service security, which ensure normal running of services.

NOTE

Enable security features based on service types. For details, see **13.2.5 Principle of Security Data Plan**.

Procedure

- Configure queue scheduling.

  Based on **13.2.3 Principle of QoS Data Plan**, all packets use strict priorities for queue scheduling and are mapped to queues based on priorities.

Copyright © Huawei Technologies Co., Ltd.

```
huawei(config)#queue-scheduler strict-priority
huawei(config)#cos-queue-map cos0 0 cos1 1 cos2 2 cos3 3 cos4 4 cos5 5 cos6 6
cos7 7  //System default
```

- Configure system security.
  - Enable deny of service (DoS) anti-attack on both the OLT and optical network units (ONUs).
    1. Run the **security anti-dos enable** command to globally enable DoS anti-attack.
    2. Run the **security anti-dos control-packet policy** command to configure a protocol packet processing policy that will be used when a DoS attack occurs.
    3. Run the **security anti-dos control-packet rate** command to configure the threshold for the rate of sending protocol packets to the CPU.
  - Enable IP address anti-attack on both the OLT and ONUs.

    Run the **security anti-ipattack enable** command to enable IP address anti-attack.
- Configure user security.
  - Enable MAC address anti-flapping on both the OLT and ONUs.

    Run the **security anti-macduplicate enable** command to enable MAC address anti-flapping.
  - Enable MAC address anti-spoofing on both the OLT and ONUs.
    1. In global config mode, run the **security anti-macspoofing enable** command to globally enable MAC address anti-spoofing.
    2. Enable MAC address anti-spoofing at VLAN level in global config mode or service profile mode:
       a. In global config mode, run the **security anti-macspoofing vlan** command to enable MAC address anti-spoofing.
       b. Perform the following operations to enable MAC address anti-spoofing in service profile mode:
          a. In global config mode, run the **vlan service-profile** command to create a VLAN service profile.
          b. Run the **security anti-macspoofing enable** command to enable MAC address anti-spoofing at VLAN level.
          c. Run the **commit** command to make the profile configuration take effect.
          d. Run the **quit** command to quit the VLAN service profile mode.
          e. Run the **vlan bind service-profile** command to bind the created VLAN service profile to a VLAN.
    3. (Optional) Run the **security anti-macspoofing max-mac-count** command to set the maximum number of MAC addresses that can be bound to a service flow.
    4. (Optional) Run the **security anti-macspoofing exclude** command to configure the types of packets for which MAC address anti-spoofing does not take effect, such as Internet Group Management Protocol (IGMP) packets.
  - Enable IP address anti-spoofing on ONUs.

    IP address anti-spoofing can be enabled or disabled at three levels: global, VLAN, and service port levels. This function takes effect only after it is enabled at the three levels. Among the three levels, IP address anti-spoofing is disabled only at the global level by default.

Copyright © Huawei Technologies Co., Ltd.

1. In global config mode, run the **security anti-ipspoofing enable** command to enable IP address anti-spoofing at the global level.
2. In VLAN service profile mode, run the **security anti-ipspoofing enable** command to enable IP address anti-spoofing at the VLAN level.
3. Run the **security anti-ipspoofing service-port** *serviceport-id* **enable** command to enable IP address anti-spoofing at the service port level.

----End

14.4.1.8 Configuring Network Protection

The base station access service has high requirements on reliability. Therefore, network protection solutions must be configured in the upstream and downstream directions.

Context

- The upstream protection solution is STM-1 1+1 protection (OLTs must transmit services upstream through STM-1 ports).
- The downstream protection solutions are Type B protection and Type C single-homing protection. For details on configurations, see **13.3.1.8 Configuring E2E Reliability**. The following uses Type C single-homing protection as an example.

Procedure

- Configure an STM-1 protection group.

  Configure STM-1 ports 0/5/0 and 0/5/1 on the TOPA board as members in the same protection group. When a hardware or line fault occurs at the protected port 0/5/0, the system automatically switches services at the faulty port to the standby port 0/5/1.

```
huawei(config)#protect-group 1 protect-target stm-nni-port workmode
unidirection
huawei(protect-group-0)#protect-group member port 0/5/0 role work
huawei(protect-group-0)#protect-group member port 0/5/1 role protect
huawei(protect-group-0)#protect-group enable
```

NOTICE

OLTs only support unidirectional STM-1 protection. When OLTs are interconnected with SDH equipment, the STM-1 protection mode of the remote SDH equipment must be set to unidirectional.

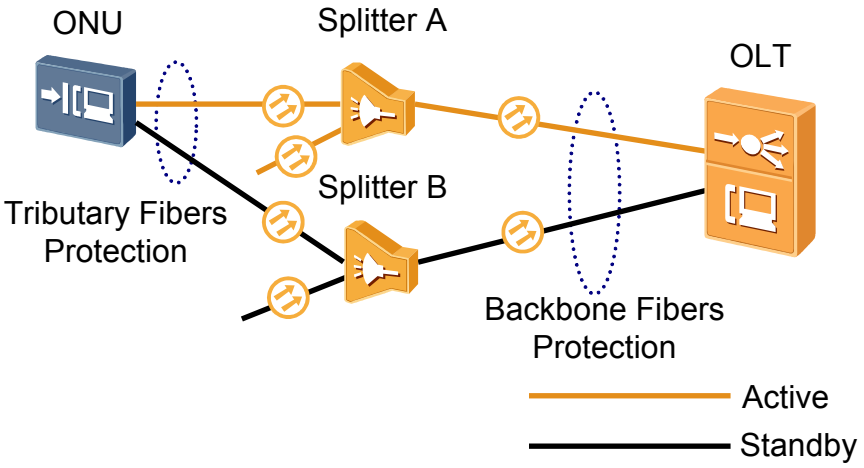
- Configure the Type C single homing protection.

  Figure 14-8 shows networking diagram for the Type C single homing protection. Configure two 1:N optical splitters, one for connecting the working PON ports on the OLT and ONUs, and one for connecting the protection PON ports on the OLT and ONUs. This protection scheme protects both the backbone fibers and tributary fibers.

  The configurations of services accessed by the ONUs remain the same after the Type C single homing protection is configured. That is, the service configurations are applied only to the working PON port on the OLT and working upstream PON ports on the ONUs.

Copyright © Huawei Technologies Co., Ltd.

Figure 14-8 Type C single homing protection



As shown in the preceding figure, Type C single homing protecting is configured for optical fiber links between the OLT and ONU.

- The ports on the GPON service board are 0/3/1 and 0/3/2.
- The link at port 0/3/1 is the working link.
- The link at port 0/3/2 is the protection link.
- The ONU ID is 1.
- The ONU is authenticated by serial number (SN). The SN of the ONU is 32303131B39FD641 and the management mode is SNMP.
- The ID of the line profile bound to the ONU is 10.

```
huawei(config)#interface gpon 0/3
huawei(config-if-gpon-0/3)#ont add 1 1 sn-auth 32303131B39FD641 snmp ont-
lineprofile-id 10
huawei(config-if-gpon-0/3)#ont add 2 1 protect-side
huawei(config-if-gpon-0/3)#quit
huawei(config)#protect-group protect-target gpon-uni-ont workmode portstate
huawei(protect-group-1)#protect-group member port 0/3/1 ont 1 role work
huawei(protect-group-1)#protect-group member port 0/3/2 ont 1 role protect
huawei(protect-group-1)#protect-group enable
huawei(protect-group-1)#quit
```

----End

14.4.1.9 Verifying Services

This topic describes how to use the PDH/SDH tester to verify the private line access service.

Prerequisites

The private line service has been configured.

Copyright © Huawei Technologies Co., Ltd.

Networking

Figure 14-9 Test setup for E1 upstream service

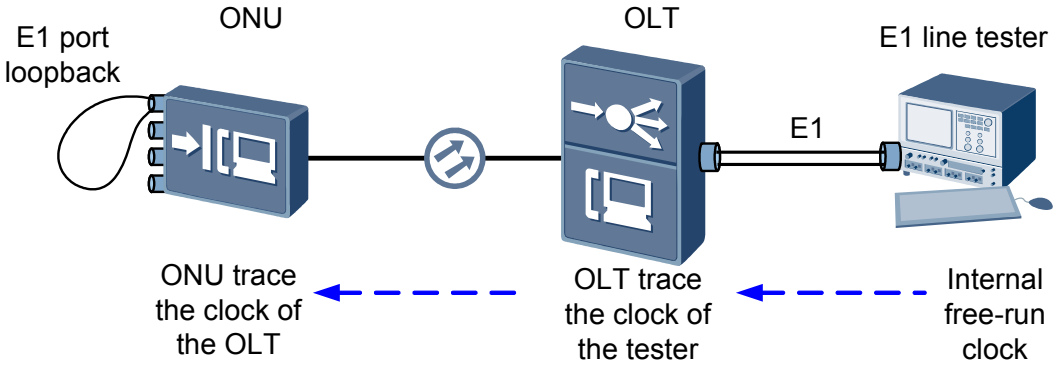
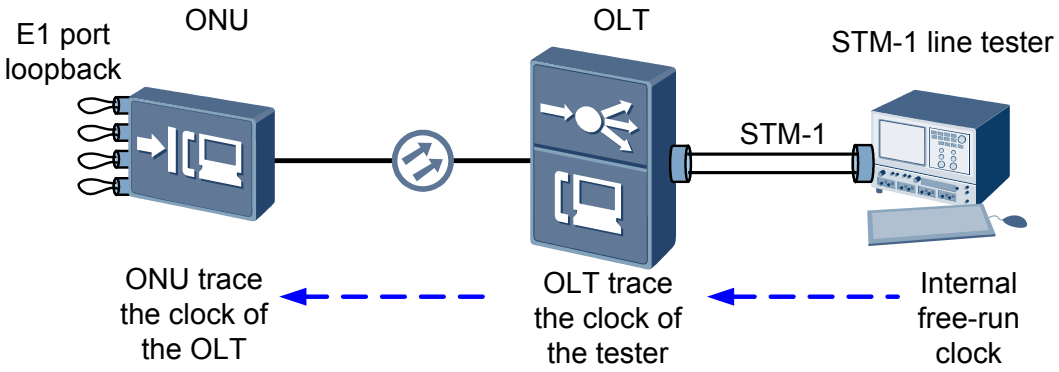


Figure 14-10 Test setup for STM-1 upstream service



Procedure

Step 1 Set up network environment according to the preceding diagrams for service acceptance tests.

NOTE

Ensure clock synchronization for the test. It is recommended that the tester use the internal free-run clock, the OLT trace the clock of the tester, and the ONU trace the clock of the OLT.

Step 2 Use the E1 or STM-1 line tester to send packets for the test.

The test duration must be 12 hours or longer. There should be no alarms on the tester and the bit error rate must be less than 1E-9.

----End

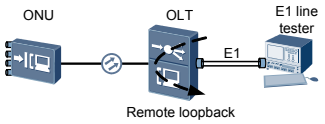
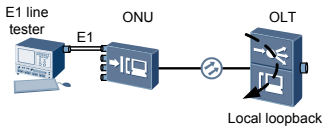
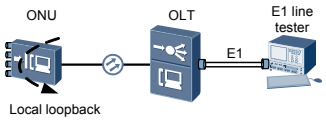
Follow-up Procedure

When the test on service connectivity fails, you can check for the failure causes by performing loopbacks. The following loopbacks are supported:

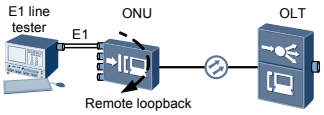
- Remote loopback on the OLT TOPA board
- Local loopback on the OLT TOPA board
- Local loopback on the ONU

Copyright © Huawei Technologies Co., Ltd.

- Remote loopback on the ONU

Loopback Mode	Function	Networking	Configuration
Remote loopback on the TOPA board	Loops back signals to the network side on the TOPA board on the OLT. This loopback checks whether the service from the TOPA board to the network-side channel is normal.		Enable/Disable the remote loopback for the E1 port. huawei(config)#**interface top 0/5** huawei(config-if-top-0/5)#**loopback 0 remote** huawei(config-if-top-0/5)#**undo loopback 0** Enable/Disable the remote loopback for the STM-1 port. huawei(config)#**interface top-stm1 0/5** huawei(config-if-top-stm1-0/5)#**loopback 0 remote** huawei(config-if-top-stm1-0/5)#**undo loopback 0**
Local loopback on the TOPA board	Loops back signals to the user side on the TOPA board on the OLT. This loopback checks whether the link between the TOPA board and the E1 port on the ONU is normal.		Enable/Disable the local loopback for the E1 port. huawei(config)#**interface top 0/5** huawei(config-if-top-0/5)#**loopback 0 local** huawei(config-if-top-0/5)#**undo loopback 0** Enable/Disable the local loopback for the STM-1 port. huawei(config)#**interface top-stm1 0/5** huawei(config-if-top-stm1-0/5)#**loopback 0 local** huawei(config-if-top-stm1-0/5)#**undo loopback 0**
Local loopback on the ONU	Loops back signals to the network side on the ONU. This loopback checks whether the link between the E1 port on the ONU and the TOPA board on the OLT is normal.		huawei(config)#**interface tdm** huawei(config-if-tdm-)#**loopback 0 local** huawei(config-if-tdm-)#**undo loopback 0**

Copyright © Huawei Technologies Co., Ltd.

Loopback Mode	Function	Networking	Configuration
Remote loopback on the ONU	Loops back signals to the user side on the ONU. This loopback checks whether the link between the ONU and user terminal is normal.		huawei(config)#**interface tdm** huawei(config-if-tdm-)#**loopback 0 remote** huawei(config-if-tdm-)#**undo loopback 0**

14.4.2 E1 Base Station Access Service (in SAToP Mode)

ONUs transmit E1 signals of base stations to OLTs in SAToP mode and OLTs are interconnected with transmission equipment through E1 ports. In this manner, traditional circuit switching services can be carried over GPON networks.

14.4.2.1 Service Requirement and Application Scenario

Service Requirement

As a mainstream full-service access technology in the future, the passive optical network (PON) supports fast deployment and service provisioning. It also helps simplify the access network and reduce the costs on construction and subsequent maintenance of the access network. Currently, carriers in China and outside China are using the PON to carry 2G/3G base station services over their existing FTTx networks that are established for accessing individual/enterprise users. In this manner, carriers can implement the access of all the services at the access layer in an unified mode.

- ONUs are connected to 2G or 3G base stations through E1/T1 ports.
- GPON is used for carrying the mobile access network in a unified manner to meet mobile carriers' requirements for a high bandwidth and high-density coverage of base stations.
- Existing SDH resources are utilized efficiently to implement high-quality transmission of TDM services.

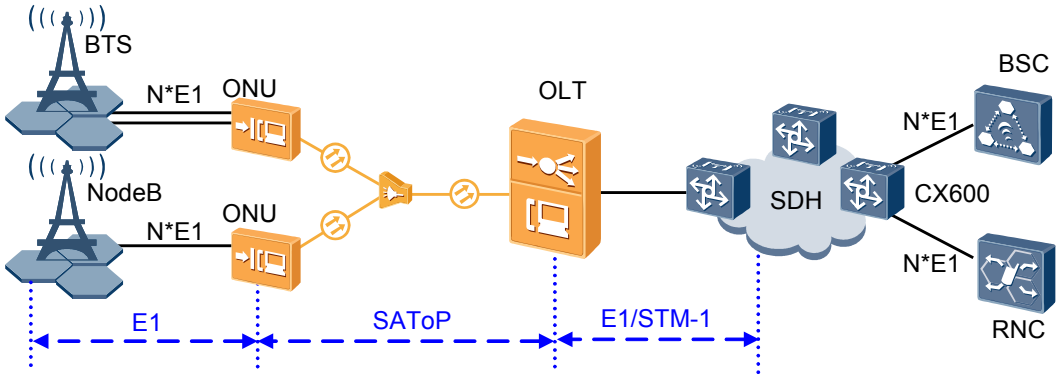
Application Scenario

As shown in **Figure 14-11**, the ONU accesses E1/T1 services of the 2G or 3G base station through the unified hardware port, and then transmits the service data to the OLT in the SAToP mode. The OLT restores E1/T1 signals, and then transmits the signals to the SDH network through the E1/T1 port. In this manner, service access of the 2G or 3G base station is implemented between the ONU and the OLT in the SAToP mode.

Applicable ONUs: MA5612, MA5628, MA5616

Copyright © Huawei Technologies Co., Ltd.

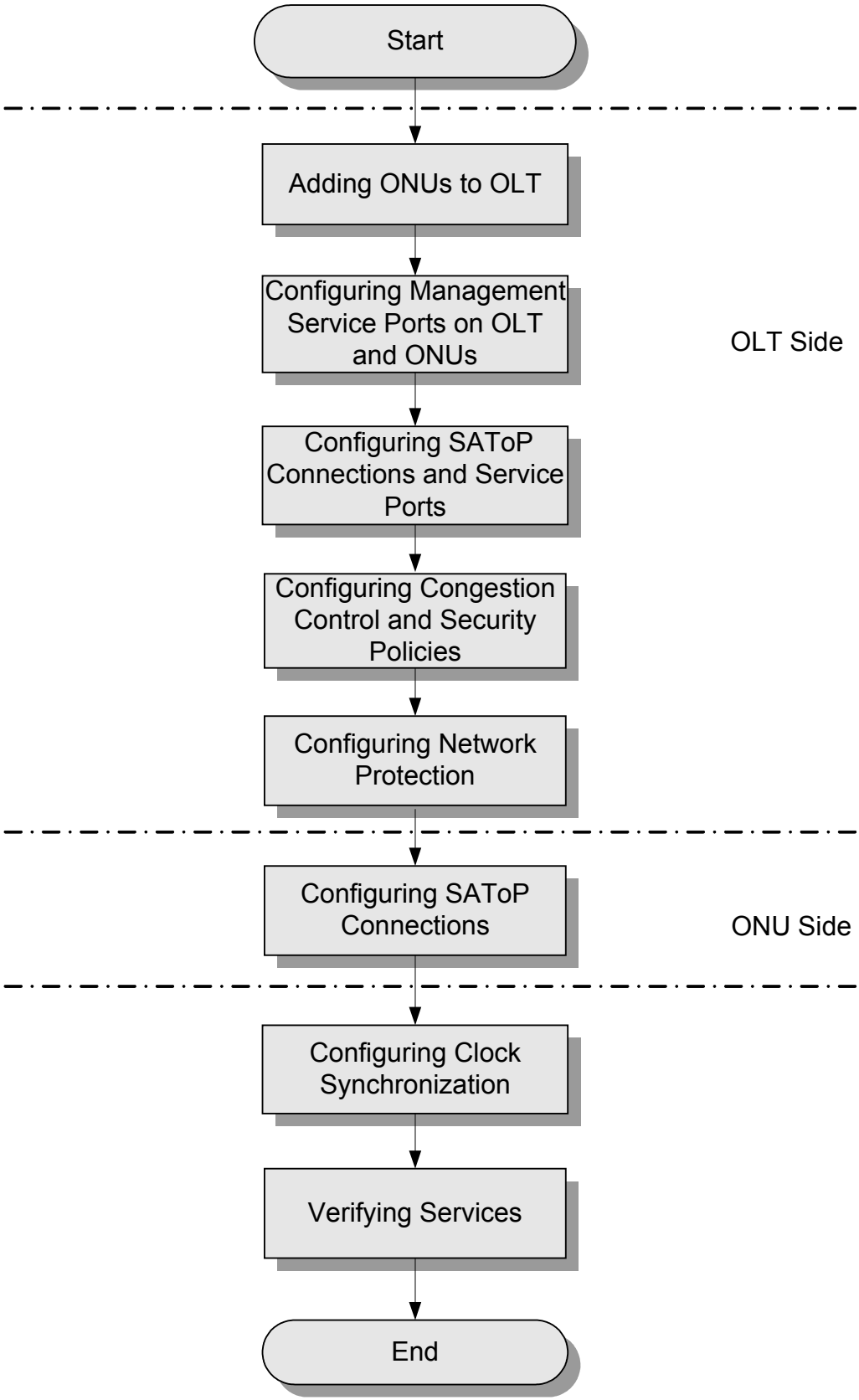
Figure 14-11 Networking diagram of E1/T1 base station access service



14.4.2.2 Configuration Process

The following figure shows the configuration process for E1/T1 base station access service (in SAToP mode).

Copyright © Huawei Technologies Co., Ltd.



Copyright © Huawei Technologies Co., Ltd.

14.4.2.3 Adding ONUs to OLT

ONUs can be configured only after they are added to the OLT successfully.

Context

- When adding ONUs, you need to bind related profiles to the ONUs, including the DBA profile, line profile, and alarm profile.
- An ONU can be added in two modes: offline addition and online confirmation. Select either mode as required.

Data Plan

Table 14-4 Key data plan

Item	Data
DBA profile	Profile ID: 20 Profile type: Fixed bandwidth and minimum delay DBA bandwidth: ● E1 access: 32 Mbit/s is recommended. (Each ONU accesses four E1 private lines and each line has a recommended DBA bandwidth of 8 Mbit/s) ● T1 access: 24 Mbit/s is recommended. (Each ONU accesses four T1 private lines and each line has a recommended DBA bandwidth of 6 Mbit/s)
Line profile	Profile ID: 10 T-CONT ID: 1 GEM port ID for management service: 11 GEM port ID for DDN private line service: 12
Networking data	PON port: 0/3/1 ONU parameters: ● ONU ID: 1 ● SN: 32303131B39FD641

Procedure

Step 1 Configure GPON ONU profiles.

1. Configure a DBA profile. and set the DBA bandwidth allocation mode for the GPON port to minimum bandwidth delay.

   For example, configure the DBA profile for 4-channel E1 private line.

```
huawei(config)#dba-profile add profile-id 20 type1 fix 32768
huawei(config)#interface gpon 0/3
huawei(config-if-gpon-0/3)#port dba bandwidth-assignment-mode 1 min-loop-delay
huawei(config-if-gpon-0/3)#quit
```


Copyright © Huawei Technologies Co., Ltd.

2. Configure an ONU line profile.

```
huawei(config)#ont-lineprofile gpon profile-id 10
huawei(config-gpon-lineprofile-10)#tcont 1 dba-profile-id 20  //Bind T-CONT 1
to DBA profile 20
huawei(config-gpon-lineprofile-10)#gem add 11 eth tcont 0
huawei(config-gpon-lineprofile-10)#gem add 12 eth tcont 1 //Add GEM port 12 to
T-CONT 1
huawei(config-gpon-lineprofile-10)#gem mapping 11 0 vlan 8
huawei(config-gpon-lineprofile-10)#gem mapping 12 1 vlan 300 //Map GEM port 12
to CVLAN 300
huawei(config-gpon-lineprofile-10)#commit
huawei(config-gpon-lineprofile-10)#quit
```

3. (Optional) Configure an alarm profile.
   - The default GPON alarm profile ID is 1. The value of each alarm threshold is **0** which indicates that alarms are not reported.
   - In this example, the default alarm profile is used and no configuration is required.

Step 2 Add ONUs to the OLT.

1. Add ONU 1 in offline mode.

```
huawei(config)#interface gpon 0/3
huawei(config-if-gpon-0/3)#ont add 1 ontid 1 sn-auth 32303131B39FD641
snmp ont-lineprofile-id 10
```

2. (Optional) Bind an alarm profile.

   By default, an ONU will be automatically bound to alarm profile 1 (default profile). You need to manually bind an alarm profile to an ONU only when the default alarm profile does not meet requirements.

   In this example, the default alarm profile is used. Therefore, you do not need to manually bind an alarm profile.

Step 3 Confirm the ONU status.

After adding an ONU, run the **display ont info** command to query the current status of the ONU. Ensure that **Control flag** is **active**, **Run State** is **online**, and **Config state** is **normal**.

The following uses ONU 1 as an example to describe how to confirm ONU status.

```
huawei(config-if-gpon-0/3)#display ont info 1 1
  ------------------------------------------------------------------------
  F/S/P                : 0/3/1
  ONT-ID               : 1
  Control flag         : active    //Indicates that the ONU is
activated.
  Run state            : online    //Indicates that the ONU is
online.
  Config state         : normal    //Indicates that the ONU is in normal
state.
...//Other command output is omitted.
huawei(config-if-gpon-0/3)#quit
```

----End

Follow-up Procedure

When **Config state** is **failed**, **Run state** is **offline**, or **Match state** is **mismatch**:

- If **Control flag** is **deactive**, run the **ont active** command in GPON mode to activate the ONU.

Copyright © Huawei Technologies Co., Ltd.

- If **Run state** is **offline**, a physical line may be broken or the optical module may be damaged. Check the line and the optical module.
- If **Config state** is **failed**, the configured ONU capability exceeds the actual ONU capability. In this case, run the **display ont failed-configuration** command in the diagnose mode to check the failed configuration item and the failure cause. Then, rectify the fault accordingly.
- If the ONU does not match, that is, **Match state** is **mismatch**, the port types and number of ports undermatch the actual port types and number of ports supported by the ONU. In this case, run the **display ont capability** command to query the actual capability of the ONU, and then select one of the following modes to modify the ONU configuration:
  - Create a proper ONU profile according to the actual capability of the ONU, and then run the **ont modify** command to modify the configuration data of the ONU.
  - Modify the ONU profile according to the actual capability of the ONU and save the modification. Then, the ONU automatically recovers the configuration successfully.

14.4.2.4 Configuring Management Service Ports on OLT and ONUs

This topic describes how to configure management service ports (also called service flows) on the OLT and ONUs. After the connections between the in-band management service ports on the OLT and ONUs are reachable, you can log in to the ONUs on the OLT and configure the ONUs.

Data Plan

Configuration Item	Data
Management VLAN and management IP address for OLT	Management VLAN ID: 8 Management VLAN type: smart In-band management IP address: 192.168.50.1/24
Management VLAN and management IP address for ONU	Management VLAN ID: 8 Management VLAN type: smart In-band management IP address for ONU 3: 192.168.50.2/24

Procedure

Step 1 Configure the in-band management VLAN and IP address for the OLT.

Set the in-band management VLAN to 8, VLAN priority to 6, and IP address to 192.168.50.1/24.

```
huawei(config)#vlan 8 smart
huawei(config)#port vlan 8 0/19 0
huawei(config)#vlan priority 8 6
huawei(config)#interface vlanif 8
huawei(config-if-vlanif8)#ip address 192.168.50.1 24
huawei(config-if-vlanif8)#quit
```

Step 2 Configure the in-band management VLAN and IP address for the ONU.

```
huawei(config)#interface gpon 0/3
huawei(config-if-gpon-0/3)#ont ipconfig 1 1 static ip-address 192.168.50.2 mask
```


Copyright © Huawei Technologies Co., Ltd.

```
255.255.255.0 gateway
192.168.50.1 vlan 8
huawei(config-if-gpon-0/3)#quit
```

Step 3 Configure the in-band management service port.

Set the management VLAN to 8, GEM port ID to 11, and user VLAN to 8. The OLT does not rate limit the in-band management service port. Therefore, directly use the default traffic profile 6.

```
huawei(config)#service-port vlan 8 gpon 0/3/1 ont 1 gemport 11 multi-service
user-vlan 8 rx-cttr 6 tx-cttr 6
```

Step 4 Confirm that the connection between the management service ports on the OLT and ONU is reachable.

- Run the **ping *ONU ip*** command on the OLT to verify the connectivity between the OLT and ONU. If the OLT receives ICMP ECHO-REPLY packets from the ONU, the connection is reachable.
- When the connection is reachable, you can remote log in to the ONU from the OLT and configure the ONU.

----End

14.4.2.5 Configuring SAToP Connections and Service Ports

This topic describes how to configure a SAToP connection of the IP+UDP encapsulation type and a service port to enable packets of base stations to be encapsulated on ONUs and restored on OLTs.

Prerequisites

Required hardware is available:

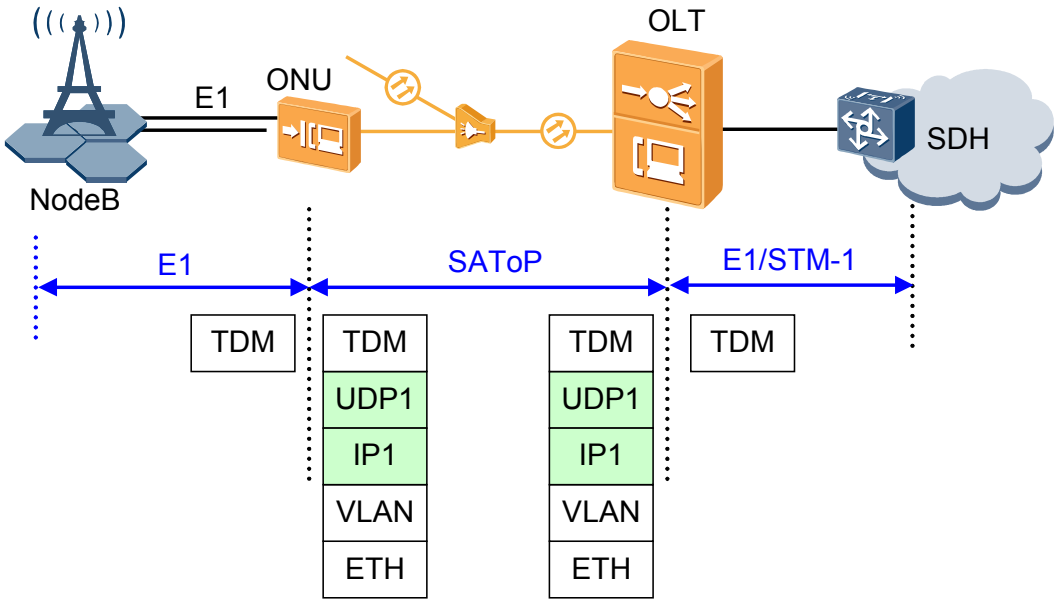
- Main control boards on the OLT: SCUN+CKMC/CKMD
- Upstream board on the OLT: EDTB (for E1 upstream transmission)
- Service board on the OLT: GPBD
- ONU: MA5612 (configured with the E81A board) or MA5628

Context

Figure 14-12 shows SAToP encapsulation for E1 base station access service. As shown in the following figure, after TDM signals are encapsulated in the IP+UDP format, an outer VLAN tag and an Ethernet header are added to the TDM signals. Then the TDM signals become a standard Ethernet packet that is transmitted on the PON line between the ONU and OLT.

Copyright © Huawei Technologies Co., Ltd.

Figure 14-12 SAToP encapsulation



Data Plan

Configuration Item	Data
EDTB (OLT)	Port: 0/5/0 Board IP address: 10.10.50.10 Board MAC address: dynamically obtained (**remark 1**) Local UDP port number: 50048 (**remark 2**)
E1 port (ONU)	Board IP address: 10.10.50.20 Board MAC address: dynamically obtained (**remark 1**) UDP port number: 50048 (**remark 2**)
VLAN	SVLAN: 300

Remark 1: MAC address configuration modes (statically configured or dynamically obtained) at two ends must be consistent to establish a SAToP connection. It is recommended that MAC addresses be dynamically obtained, which facilitates configuration and maintenance.

Remark 2: The UDP port cannot be a port that is widely used in the industry and for specific services. For example, port 80 is used for HTTP service. The dynamic and private ports are recommended.

Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Configure EDTB board attributes.

Set the board working mode to SAToP.

```
huawei(config)#interface edt 0/5
huawei(config-if-edt-0/5)#board workmode satop
```

Configure the access mode and frame format.

- E1 access:
  ```
  huawei(config-if-edt-0/5)#tdm access-mode E1
  ```

Configure the IP address of the E1 port on the EDTB board.

```
huawei(config)#interface edt 0/5
huawei(config-if-edt-0/5)#set ip-address 10.10.50.10
huawei(config-if-edt-0/5)#quit
```

Step 2 Create a SAToP connection.

Create TDM VCL 10.

- For E1 access, set the TDM VCL type to SAToP.
  ```
  huawei(config)#tdm-vcl tdm-vcl-id 10 satop 0/5/0
  ```

Create a SAToP connection at the E1 port 0/5/0. Set SVLAN to 300, local UDP port number to 50048, remote IP address (the IP address of the E1 access board on the ONU) to 10.10.50.20, and remote UDP port number to 50048. The remote MAC address is obtained dynamically.

NOTE

To create a SAToP connection, the local UDP port number must be consistent with the remote UDP port number, that is, [*local-udp* = *portid* of EDTB + Cardinal number (50048)].

```
huawei(config)#cesop-connect tdm 10 vlan 300 local-udp 50048 remote-ip 10.10.50.20
remote-udp 50048
```

You can also create a SAToP connection by configuring the MAC address statically. If the remote MAC address (the MAC address of the E1 access board on the ONU, which can be queried by running the **display cesop-mac-address** command on the ONU) is 00e0-fc01-0450, create a SAToP connection in static mode as follows:

```
huawei(config)#cesop-connect tdm 10 vlan 300 local-udp 50048 remote-mac
 00e0-fc01-0450 remote-ip 10.10.50.20 remote-udp 50048
```

Step 3 (Optional) Configure attributes of the SAToP connection.

NOTE

The attributes of the SAToP connection on the OLT must be consistent with those on the ONU. Generally, use the system default values.

- Run the **cesop rtp** command to configure whether the SAToP packet carries the RTP header. The SAToP packet carries the RTP header by default.
- Run the **cesop encap** command to configure SSRC, payload type, and SN of the SAToP packet. The default value of these parameters is **0**.
- Run the **cesop jitter-buffer** command to configure the buffer depth of the SAToP packet. The default buffer depth is 2000 μs.
- Run the **cesop loadtime** command to configure the load time of the SAToP packet. The default load time is 125 μs.
- Run the **cesop priority** command to configure the priority of the SAToP packet. The default priority is 7.

Copyright © Huawei Technologies Co., Ltd.

Step 4 Configure a service port.

Set the service port ID to 1, SVLAN ID to 300, GEM port ID to 12, and user VLAN ID to 300. The ONU limits upstream and downstream traffic rates but the OLT does not. Therefore, use default traffic profile 6.

The user VLAN must be the same as the upstream VLAN of the ONU.

```
huawei(config)#vlan 300 smart
huawei(config)#service-port 1 vlan 300 gpon 0/3/1 ont 1 gemport 12 multi-service
user-vlan 300 rx-cttr 6 tx-cttr 6
```

----End

14.4.2.6 Configuring Clock Synchronization

In this scenario, the E1/STM-1 line clock can be used to achieve network-wide clock synchronization.

Prerequisites

The CKMC/CKMD clock daughter board has been installed on the SCU main control board.

Context

Configuration roadmap for clock synchronization:

1. The OLT traces the upstream E1/STM-1 line clock of the TOPA board as the system clock.
2. The system clock is delivered to an ONU through optical paths of the GPON board.
3. The ONU uses the line clock of the GPON upstream port as the system clock.
4. The ONU E1 transmit clock is synchronized with the system clock of the ONU.

Procedure

- **Configure a clock on the OLT.**
  1. Add a system clock source.

     Configure the E1/T1 line clock input from port 0/5/0 on the EDTB board as the system clock 0. Set the priority to **0** (highest priority).

     ```
     huawei(config)#clock source 0 0/5/0
     huawei(config)#clock priority system 0
     ```

  2. Query configurations and the status of the system clock source.

     Run the **display clock source system** command to query configurations and the status of the clock source. Ensure that configurations of the system clock source are correct and the status is **Normal**.

     ```
     huawei(config)#display clock source system

     ------------------------------------------------------------------------
     -----
       Index  Board    Source   Clk-type  State       Priority QL
     Selected

     ------------------------------------------------------------------------
     -----
         0    H802EDTB 0/5/0    E1        Normal      0        ---
     YES
     ```


Copyright © Huawei Technologies Co., Ltd.

```
-------------------------------------------------------------------------
-----
```

Run the **display clock mode** command to query the clock working mode. Ensure that the clock daughter board works in tracing mode.

```
huawei(config)#display clock mode
  Clock manage-mode:Third-mode
  Clock subboard work-mode:Tracing
```

- **Configure a clock on the ONU.**

  1. Configure the GPON line clock as the system clock.

     The system clock of the OLT is delivered to the ONU through the GPON port on the OLT, achieving clock synchronization between the OLT and the ONU.

     a. Run the **clock source** command to configure the clock recovered from the GPON upstream port as the system clock of the ONU.

     b. Run the **clock priority** command to configure the priority of the clock source.

     ```
     huawei(config)#clock source 0 0/0/1
       Clock source set succeeded

     huawei(config)#clock priority system 0
     ```

  2. Configure the system clock as the transmit clock for an E1 port.

     a. Run the **interface tdm** command to enter the E1 port configuration mode.

     b. Run the **tx clock** or **port** *portid* **udt system** command to configure the system clock as the transmit clock of the port.

     c. Run the **display port state** command to query the transmit clock of the E1 port.

     ```
     huawei(config)#interface tdm
     huawei(config-if-tdm-)#port 0 udt system
     huawei(config-if-tdm-)#display port state 0
       ---------------------------------------
       Port          : 0
       State         : normal
       Mode          : UDT
       Code          : HDB3
       Looptype      : -
       Timeslot      : -
       Clock         : system
       CRC4          : -
       Signaling     : -
       ESF           : -
       Impedance     : 120 Ohm
       ---------------------------------------
     ```

  3. Query configurations and the status of the system clock source.

     Run the **display clock source** command to query configurations and the status of the system clock source.

     ```
     huawei(config-if-tdm-)#quit
     huawei(config)#display clock source
       ------------------------------------------------------------------
       Index  Config   Type   Source      State     Priority   Output
       ------------------------------------------------------------------
         0    YES      line   0/0/1       Normal    0          YES
         1    NO       --     -/ -/ -     ---       ---        ---
         2    NO       --     -/ -/ -     ---       ---        ---
         3    NO       --     -/ -/ -     ---       ---        ---
         4    NO       --     -/ -/ -     ---       ---        ---
         5    NO       --     -/ -/ -     ---       ---        ---
         6    NO       --     -/ -/ -     ---       ---        ---
         7    NO       --     -/ -/ -     ---       ---        ---
         8    NO       --     -/ -/ -     ---       ---        ---
     ```


Copyright © Huawei Technologies Co., Ltd.

```
  9     NO       --      -/ -/ -     ---         ---         ---
-------------------------------------------------------------
```

----End

14.4.2.7 Configuring Congestion Control and Security Policies

This topic describes how to configure global priority-based scheduling policies for queues to ensure service reliability and configure global security policies to ensure service security.

Context

Congestion control uses queue scheduling technology to map packets sent from the same port into multiple queues and process packets in each queue based on priority. Congestion control is recommended.

Security policies cover system security, user security, and service security, which ensure normal running of services.

NOTE

Enable security features based on service types. For details, see **13.2.5 Principle of Security Data Plan**.

Procedure

- Configure queue scheduling.

  Based on **13.2.3 Principle of QoS Data Plan**, all packets use strict priorities for queue scheduling and are mapped to queues based on priorities.

  ```
  huawei(config)#queue-scheduler strict-priority
  huawei(config)#cos-queue-map cos0 0 cos1 1 cos2 2 cos3 3 cos4 4 cos5 5 cos6 6 cos7 7  //System default
  ```

- Configure system security.
  - Enable deny of service (DoS) anti-attack on both the OLT and optical network units (ONUs).
    1. Run the **security anti-dos enable** command to globally enable DoS anti-attack.
    2. Run the **security anti-dos control-packet policy** command to configure a protocol packet processing policy that will be used when a DoS attack occurs.
    3. Run the **security anti-dos control-packet rate** command to configure the threshold for the rate of sending protocol packets to the CPU.
  - Enable IP address anti-attack on both the OLT and ONUs.

    Run the **security anti-ipattack enable** command to enable IP address anti-attack.
- Configure user security.
  - Enable MAC address anti-flapping on both the OLT and ONUs.

    Run the **security anti-macduplicate enable** command to enable MAC address anti-flapping.
  - Enable MAC address anti-spoofing on both the OLT and ONUs.
    1. In global config mode, run the **security anti-macspoofing enable** command to globally enable MAC address anti-spoofing.
    2. Enable MAC address anti-spoofing at VLAN level in global config mode or service profile mode:

Copyright © Huawei Technologies Co., Ltd.

a. In global config mode, run the **security anti-macspoofing vlan** command to enable MAC address anti-spoofing.

b. Perform the following operations to enable MAC address anti-spoofing in service profile mode:

a. In global config mode, run the **vlan service-profile** command to create a VLAN service profile.

b. Run the **security anti-macspoofing enable** command to enable MAC address anti-spoofing at VLAN level.

c. Run the **commit** command to make the profile configuration take effect.

d. Run the **quit** command to quit the VLAN service profile mode.

e. Run the **vlan bind service-profile** command to bind the created VLAN service profile to a VLAN.

3. (Optional) Run the **security anti-macspoofing max-mac-count** command to set the maximum number of MAC addresses that can be bound to a service flow.

4. (Optional) Run the **security anti-macspoofing exclude** command to configure the types of packets for which MAC address anti-spoofing does not take effect, such as Internet Group Management Protocol (IGMP) packets.

- Enable IP address anti-spoofing on ONUs.

  IP address anti-spoofing can be enabled or disabled at three levels: global, VLAN, and service port levels. This function takes effect only after it is enabled at the three levels. Among the three levels, IP address anti-spoofing is disabled only at the global level by default.

1. In global config mode, run the **security anti-ipspoofing enable** command to enable IP address anti-spoofing at the global level.

2. In VLAN service profile mode, run the **security anti-ipspoofing enable** command to enable IP address anti-spoofing at the VLAN level.

3. Run the **security anti-ipspoofing service-port** *serviceport-id* **enable** command to enable IP address anti-spoofing at the service port level.

----End

14.4.2.8 Configuring Network Protection

The base station access service has high requirements on reliability. Therefore, network protection solutions must be configured in the upstream and downstream directions.

Context

The protection solutions supported in this scenario are Type B protection and Type C single-homing protection.

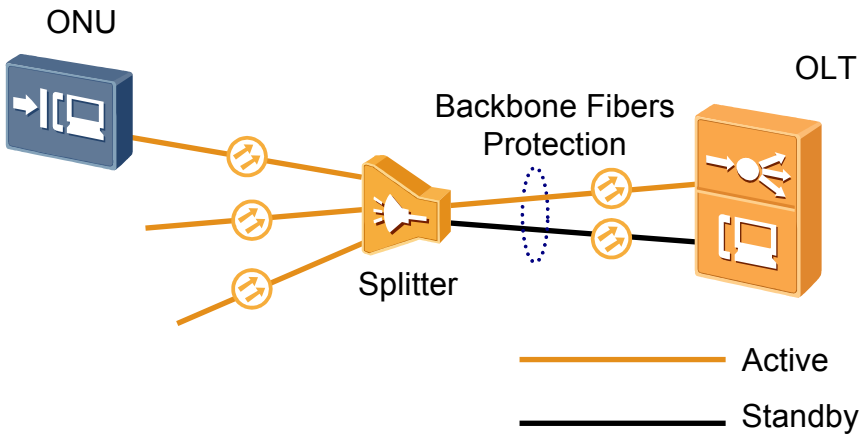
Procedure

- Configure the Type B protection.

  Figure 14-13 shows the Type B protection networking diagram.

Copyright © Huawei Technologies Co., Ltd.

Figure 14-13 Type B protection



Configure redundancy backup for ports 0/3/1 and 0/3/2 on the same GPON board on OLT. When port 0/3/1 fails, the system can automatically switch to port 0/3/2.

```
huawei(config)#protect-group 0 protect-target gpon-uni-port workmode timedelay
huawei(protect-group-0)#protect-group member port 0/3/1 role work
huawei(protect-group-0)#protect-group member port 0/3/2 role protect
huawei(protect-group-0)#protect-group enable
```

NOTE

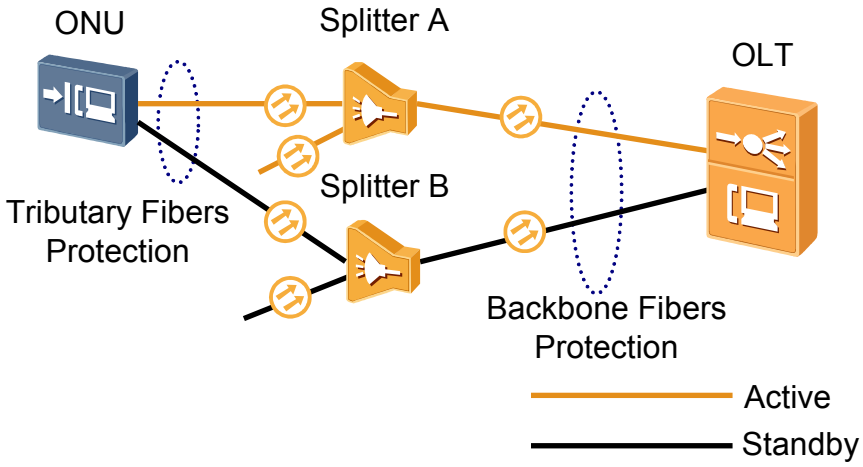
The configurations of services accessed by the ONUs remain the same after the Type B protection is configured. That is, the service configurations are applied only to the working GPON port.

- Configure the Type C single homing protection.

  Figure 14-14 shows networking diagram for the Type C single homing protection. Configure two 1:N optical splitters, one for connecting the working PON ports on the OLT and ONUs, and one for connecting the protection PON ports on the OLT and ONUs. This protection scheme protects both the backbone fibers and tributary fibers.

  The configurations of services accessed by the ONUs remain the same after the Type C single homing protection is configured. That is, the service configurations are applied only to the working PON port on the OLT and working upstream PON ports on the ONUs.

Figure 14-14 Type C single homing protection



Copyright © Huawei Technologies Co., Ltd.

As shown in the preceding figure, Type C single homing protecting is configured for optical fiber links between the OLT and ONU.

- The ports on the GPON service board are 0/3/1 and 0/3/2.
- The link at port 0/3/1 is the working link.
- The link at port 0/3/2 is the protection link.
- The ONU ID is 1.
- The ONU is authenticated by serial number (SN). The SN of the ONU is 32303131B39FD641 and the management mode is SNMP.
- The ID of the line profile bound to the ONU is 10.

```
huawei(config)#interface gpon 0/3
huawei(config-if-gpon-0/3)#ont add 1 1 sn-auth 32303131B39FD641 snmp ont-
lineprofile-id 10
huawei(config-if-gpon-0/3)#ont add 2 1 protect-side
huawei(config-if-gpon-0/3)#quit
huawei(config)#protect-group protect-target gpon-uni-ont workmode portstate
huawei(protect-group-1)#protect-group member port 0/3/1 ont 1 role work
huawei(protect-group-1)#protect-group member port 0/3/2 ont 1 role protect
huawei(protect-group-1)#protect-group enable
huawei(protect-group-1)#quit
```

----End

14.4.2.9 Configuring ONU SAToP Connections

This topic describes how to configure a SAToP connection of the IP+UDP encapsulation type and a service VLAN to enable packets of base stations to be encapsulated on ONUs as Ethernet packets and then forwarded based on VLANs and MAC addresses.

Data Plan

Configuration Item	Data
EDTB (OLT)	Port: 0/5/0 Board IP address: 10.10.50.10 Board MAC address: dynamically obtained (**remark 1**) Local UDP port number: 50048 (**remark 2**)
E1 port (ONU)	Board IP address: 10.10.50.20 Board MAC address: dynamically obtained (**remark 1**) UDP port number: 50048 (**remark 2**)
VLAN	SVLAN: 300

Remark 1: MAC address configuration modes (statically configured or dynamically obtained) at two ends must be consistent to establish a SAToP connection. It is recommended that MAC addresses be dynamically obtained, which facilitates configuration and maintenance.

Copyright © Huawei Technologies Co., Ltd.

Remark 2: The UDP port cannot be a port that is widely used in the industry and for specific services. For example, port 80 is used for HTTP service. The dynamic and private ports are recommended.

Procedure

Step 1 Configure a VLAN and add an upstream port to the VLAN.

Create the upstream VLAN 300, and add upstream port 0/0/1 to VLAN 300.

```
huawei(config)#vlan 300 smart
huawei(config)#port vlan 300 0/0 1
```

Step 2 Configure E1/T1 port attributes.

Configure the IP address of TDM service board 0/1 as 10.10.50.20.

```
huawei(config)#interface tdm 0/1
huawei(config-if-tdm-0/1)#set ip-address 10.10.50.20
```

Configure the board and port working mode and transmit clock.

- For E1 access, set the working mode to UDT and configure the transmit clock as the system clock.

```
huawei(config-if-tdm-0/1)#tdm access-mode E1
huawei(config-if-tdm-0/1)#port 0 udt system
```

Step 3 Create a SAToP connection.

Create TDM VCL 10.

- For E1 access, set the TDM VCL type to SAToP.

```
huawei(config)#tdm-vcl tdm-vcl-id 10 satop 0/1/0
```

Create a SAToP connection at TDM port 0/1/0. Set SVLAN to 300, local UDP port number to 50048, remote IP address (the IP address of the EDTB board on the OLT) to 10.10.50.10, and remote UDP port number to 50048. The remote MAC address is obtained dynamically.

```
huawei(config)#cesop-connect tdm 10 vlan 300 local-udp 50048 remote-ip 10.10.50.10
remote-udp 50048
```

NOTE

You can also create a SAToP connection by configuring the MAC address statically. If the remote MAC address (the MAC address of the EDTB board on the OLT) is 0800-3E32-5310, create a SAToP connection in static mode as follows:

```
huawei(config)#cesop-connect tdm 10 vlan 300 local-udp 50048 remote-mac
 0800-3E32-5310 remote-ip 10.10.50.10 remote-udp 50048
```

Step 4 (Optional) Configure attributes of the SAToP connection.

NOTE

The attributes of the SAToP connection on the OLT must be consistent with those on the ONU. Generally, use the system default values.

- Run the **cesop rtp** command to configure whether the SAToP packet carries the RTP header. The SAToP packet carries the RTP header by default.
- Run the **cesop encap** command to configure SSRC, payload type, and SN of the SAToP packet. The default value of these parameters is **0**.
- Run the **cesop jitter-buffer** command to configure the buffer depth of the SAToP packet. The default buffer depth is 2000 μs.

Copyright © Huawei Technologies Co., Ltd.

- Run the **cesop loadtime** command to configure the load time of the SAToP packet. The default load time is 125 μs.
- Run the **cesop priority** command to configure the priority of the SAToP packet. The default priority is 7.

----End

14.4.2.10 Verifying Services

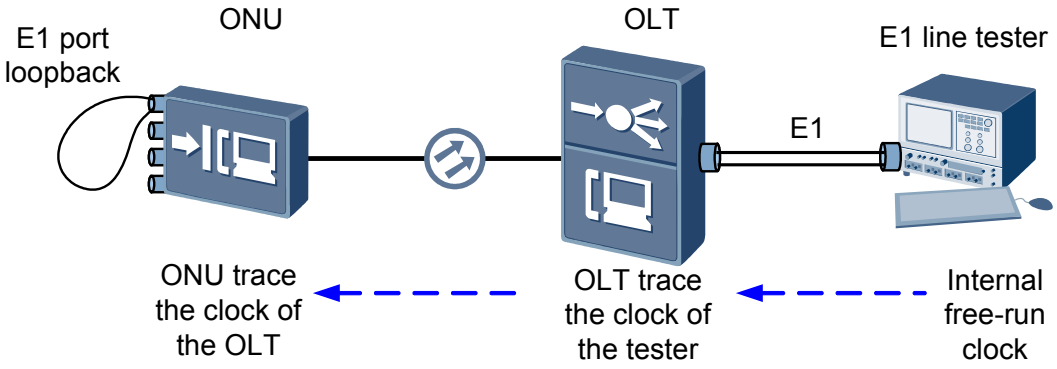
This topic describes how to use the PDH/SDH tester to verify the private line access service.

Prerequisites

The private line service has been configured.

Networking

Figure 14-15 Test setup for E1 upstream service



Procedure

Step 1 Set up network environment according to the preceding diagrams for service acceptance tests.

NOTE

Ensure clock synchronization for the test. It is recommended that the tester use the internal free-run clock, the OLT trace the clock of the tester, and the ONU trace the clock of the OLT.

Step 2 Use the E1 line tester to send packets for the test.

The test duration must be 12 hours or longer. There should be no alarms on the tester and the bit error rate must be less than 1E-9.

----End

Follow-up Procedure

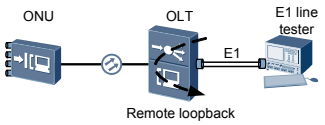
When the test on service connectivity fails, you can check for the failure causes by performing loopbacks. The following loopbacks are supported:

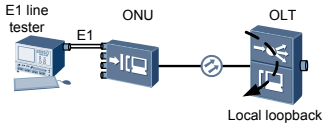
- Remote loopback on the OLT EDTB board
- Local loopback on the OLT EDTB board

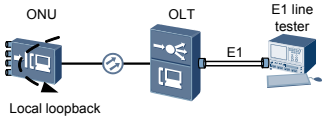
Copyright © Huawei Technologies Co., Ltd.

- Local loopback on the ONU
- Remote loopback on the ONU

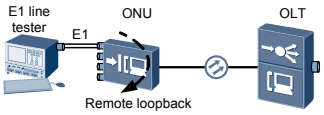
Loopback Mode	Function	Networking	Configuration

Remote loopback on the EDTB board	Loops back signals to the network side on the EDTB board on the OLT. This loopback checks whether the service from the EDTB board to the network-side channel is normal.		Enable/Disable the remote loopback for the E1 port.
			`huawei(config)#interface edt 0/5`
			`huawei(config-if-edt-0/5)#loopback 0 remote`
			`huawei(config-if-edt-0/5)#undo loopback 0`

Local loopback on the EDTB board	Loops back signals to the user side on the EDTB board on the OLT. This loopback checks whether the link between the EDTB board and the E1 port on the ONU is normal.		Enable/Disable the local loopback for the E1 port.
			`huawei(config)#interface edt 0/5`
			`huawei(config-if-edt-0/5)#loopback 0 local`
			`huawei(config-if-edt-0/5)#undo loopback 0`

Local loopback on the ONU	Loops back signals to the network side on the ONU. This loopback checks whether the link between the E1 port on the ONU and the EDTB board on the OLT is normal.		`huawei(config)#interface tdm`
			`huawei(config-if-tdm-)#loopback 0 local`
			`huawei(config-if-tdm-)#undo loopback 0`

Copyright © Huawei Technologies Co., Ltd.

Loopback Mode	Function	Networking	Configuration
Remote loopback on the ONU	Loops back signals to the user side on the ONU. This loopback checks whether the link between the ONU and user terminal is normal.		huawei(config)#**interface tdm** huawei(config-if-tdm-)#**loopback 0 remote** huawei(config-if-tdm-)#**undo loopback 0**

14.4.3 Ethernet Base Station Access Service (in QinQ VLAN Mode)

ONUs are connected to IP base stations through FE/GE Ethernet ports and OLTs are interconnected with MAN equipment in QinQ VLAN mode to achieve access of base station services.

14.4.3.1 Service Requirement and Application Scenario

Service Requirement

- ONUs are connected to 3G/LTE base stations and GPON is used for carrying the mobile access network in a unified manner to meet mobile carriers' requirements for a high bandwidth and high-density coverage of base stations.
- A simple, mature solution is used for service configuration to ensure high service quality as well as high transmission efficiency.

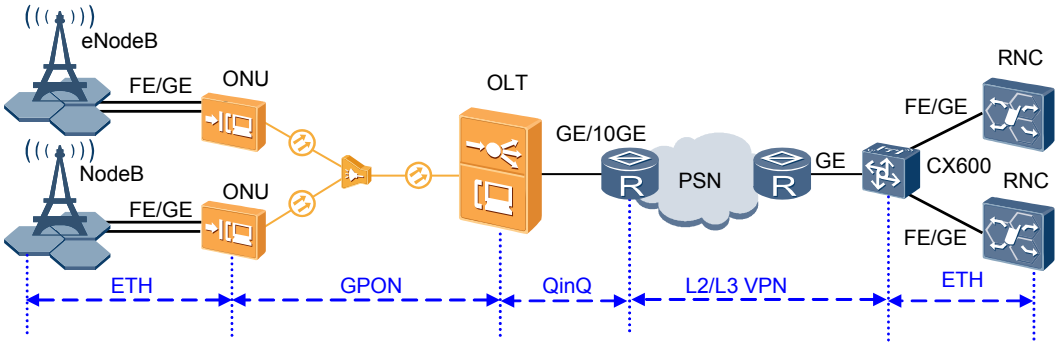
Application Scenario

As shown in **Figure 14-16**, ONUs receive the ETH service data from 3G base stations through FE/GE ports, encapsulate the ETH packets into GEM frames, and then send them to the OLT through the GPON upstream ports. The OLT restores the ETH signals and configures QinQ VLANs for the signals to enable the data of base stations to be transparently transmitted to the remote PTN over the public network. Then the remote PTN device restores the ETH signals.

Applicable ONUs: MA5612, MA5628, MA5616

Copyright © Huawei Technologies Co., Ltd.

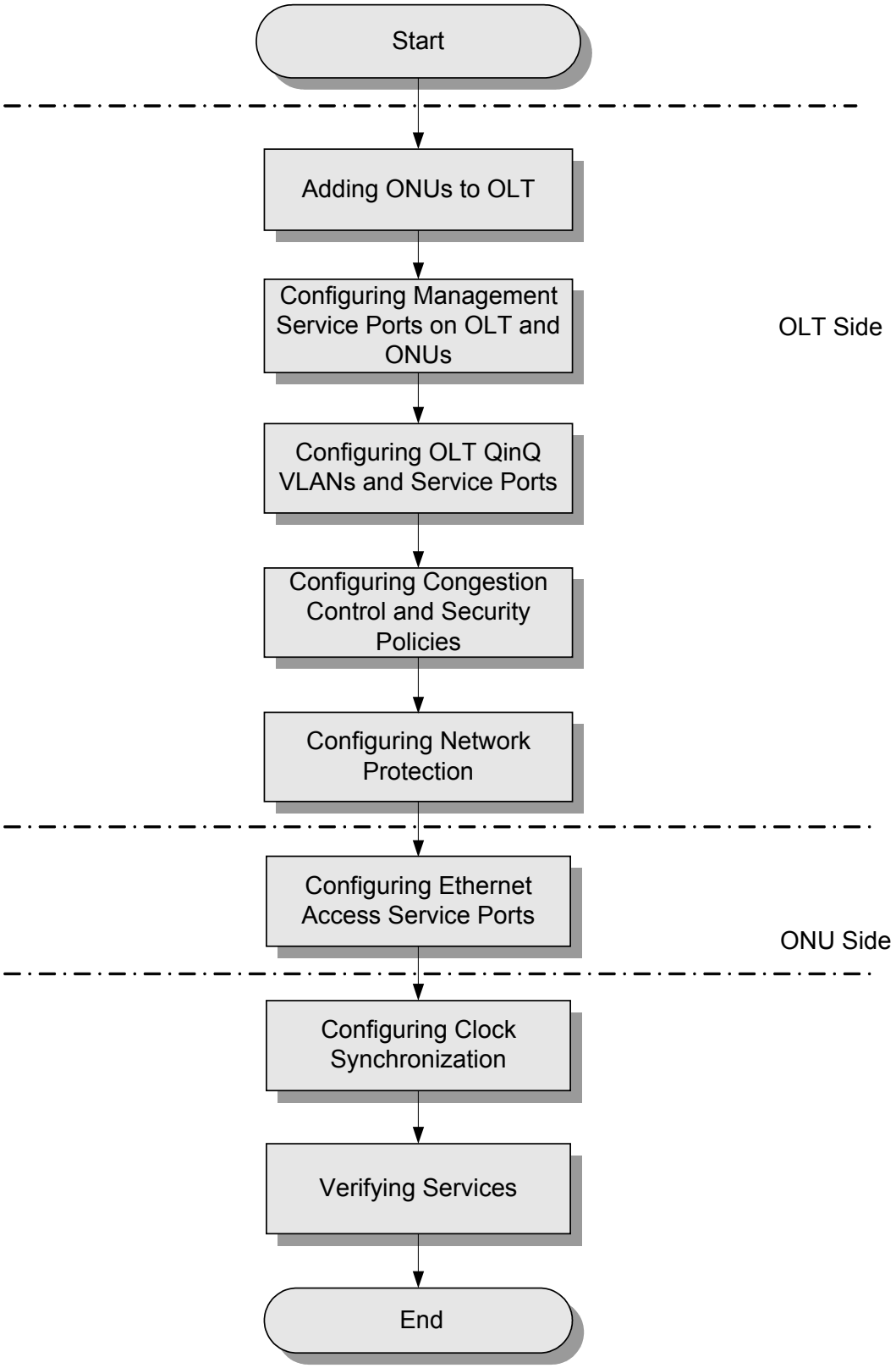
Figure 14-16 Networking diagram of Ethernet base station access service



14.4.3.2 Configuration Process

The following figure shows the configuration process for Ethernet base station access service (in QinQ VLAN mode).

Copyright © Huawei Technologies Co., Ltd.



14.4.3.3 Adding ONUs to OLT

This topic describes how to add ONUs to the OLT. ONUs can be configured only after they are added to the OLT successfully.

Copyright © Huawei Technologies Co., Ltd.

Context

- When adding ONUs, you need to bind related profiles to the ONUs, including the DBA profile, line profile, and alarm profile.
- An ONU can be added in two modes: offline addition and online confirmation. Select either mode as required.

Data Planning

Table 14-5 Key data plan

Configuration Item	Data
DBA profile	Profile ID: 20 Profile type: Type 3 Assured bandwidth: 100 Mbit/s Maximum bandwidth: 120 Mbit/s
Line profile	Profile ID: 10 T-CONT ID: 4 GEM port ID for management service of ONUs: 11 GEM Port ID for synchronization service of base stations: 12 GEM Port ID for OAM service of base stations: 13 GEM Port ID for voice and data services of base stations: 14
VLAN (remark 1)	VLAN for management service of ONUs: 8 VLAN for base station access service: ● VLAN for synchronization service: 1000 ● VLAN for OAM service: 1001 ● VLAN for voice and data services: 1002
Networking data	PON port: 0/3/1 ONU parameters: ● ONU ID: 1 ● SN: 32303131B39FD641

Remark 1: Ethernet base stations have multiple services and different services require different VLANs. The preceding table uses the synchronization service, OAM service, and voice and data services as an example.

Procedure

Step 1 Configure GPON ONU profiles.

1. Configure a DBA profile.

Copyright © Huawei Technologies Co., Ltd.

```
huawei(config)#dba-profile add profile-id 20 type3 assure 102400 max 122880
```

2. Configure an ONU line profile.

```
huawei(config)#ont-lineprofile gpon profile-id 10
huawei(config-gpon-lineprofile-10)#tcont 4 dba-profile-id 20  //Bind T-CONT 4
to DBA profile 20.
huawei(config-gpon-lineprofile-10)#gem add 11 eth tcont 0
huawei(config-gpon-lineprofile-10)#gem add 12 eth tcont 4 //Add GEM port 12 to
T-CONT 4.
huawei(config-gpon-lineprofile-10)#gem add 13 eth tcont 4 //Add GEM port 13 to
T-CONT 4.
huawei(config-gpon-lineprofile-10)#gem add 14 eth tcont 4 //Add GEM port 14 to
T-CONT 4.
huawei(config-gpon-lineprofile-10)#gem mapping 11 0 vlan 8
huawei(config-gpon-lineprofile-10)#gem mapping 12 1 vlan 1000 //Map GEM port
12 to CVLAN 1000.
huawei(config-gpon-lineprofile-10)#gem mapping 13 2 vlan 1001 //Map GEM port
13 to CVLAN 1001.
huawei(config-gpon-lineprofile-10)#gem mapping 14 3 vlan 1002 //Map GEM port
14 to CVLAN 1002.
huawei(config-gpon-lineprofile-10)#commit
huawei(config-gpon-lineprofile-10)#quit
```

3. (Optional) Configure an alarm profile.
   - The default GPON alarm profile ID is 1. The value of each alarm threshold is **0** which indicates that alarms are not reported.
   - In this example, the default alarm profile is used and no configuration is required.

Step 2 Add ONUs to the OLT.

1. Add ONU 1 in offline mode.

```
huawei(config)#interface gpon 0/3
huawei(config-if-gpon-0/3)#ont add 1 ontid 1 sn-auth 32303131B39FD641
snmp ont-lineprofile-id 10
```

2. (Optional) Bind an alarm profile.

   By default, an ONU will be automatically bound to alarm profile 1 (default profile). You need to manually bind an alarm profile to an ONU only when the default alarm profile does not meet requirements.

   In this example, the default alarm profile is used. Therefore, you do not need to manually bind an alarm profile.

Step 3 Confirm the ONU status.

After adding an ONU, run the **display ont info** command to query the current status of the ONU. Ensure that **Control flag** is **active**, **Run State** is **online**, and **Config state** is **normal**.

The following uses ONU 1 as an example to describe how to confirm ONU status.

```
huawei(config-if-gpon-0/3)#display ont info 1 1
  ------------------------------------------------------------------------
  F/S/P                : 0/3/1
  ONT-ID               : 1
  Control flag         : active    //Indicates that the ONU is
activated.
  Run state            : online    //Indicates that the ONU is
online.
  Config state         : normal    //Indicates that the ONU is in normal
state.
...//Other command output is omitted.
huawei(config-if-gpon-0/3)#quit
```

----End

Copyright © Huawei Technologies Co., Ltd.

Follow-up Procedure

When **Config state** is **failed**, **Run state** is **offline**, or **Match state** is **mismatch**:

- If **Control flag** is **deactive**, run the **ont active** command in GPON mode to activate the ONU.
- If **Run state** is **offline**, a physical line may be broken or the optical module may be damaged. Check the line and the optical module.
- If **Config state** is **failed**, the configured ONU capability exceeds the actual ONU capability. In this case, run the **display ont failed-configuration** command in the diagnose mode to check the failed configuration item and the failure cause. Then, rectify the fault accordingly.
- If the ONU does not match, that is, **Match state** is **mismatch**, the port types and number of ports undermatch the actual port types and number of ports supported by the ONU. In this case, run the **display ont capability** command to query the actual capability of the ONU, and then select one of the following modes to modify the ONU configuration:
  - Create a proper ONU profile according to the actual capability of the ONU, and then run the **ont modify** command to modify the configuration data of the ONU.
  - Modify the ONU profile according to the actual capability of the ONU and save the modification. Then, the ONU automatically recovers the configuration successfully.

14.4.3.4 Configuring Management Service Ports on OLT and ONUs

This topic describes how to configure management service ports (also called service flows) on the OLT and ONUs. After the connections between the in-band management service ports on the OLT and ONUs are reachable, you can log in to the ONUs on the OLT and configure the ONUs.

Data Plan

Configuration Item	Data
Management VLAN and management IP address for OLT	Management VLAN ID: 8 Management VLAN type: smart In-band management IP address: 192.168.50.1/24
Management VLAN and management IP address for ONU	Management VLAN ID: 8 Management VLAN type: smart In-band management IP address for ONU 3: 192.168.50.2/24

Procedure

Step 1 Configure the in-band management VLAN and IP address for the OLT.

Set the in-band management VLAN to 8, VLAN priority to 6, and IP address to 192.168.50.1/24.

```
huawei(config)#vlan 8 smart
huawei(config)#port vlan 8 0/19 0
huawei(config)#vlan priority 8 6
```


Copyright © Huawei Technologies Co., Ltd.

```
huawei(config)#interface vlanif 8
huawei(config-if-vlanif8)#ip address 192.168.50.1 24
huawei(config-if-vlanif8)#quit
```

Step 2 Configure the in-band management VLAN and IP address for the ONU.

```
huawei(config)#interface gpon 0/3
huawei(config-if-gpon-0/3)#ont ipconfig 1 1 static ip-address 192.168.50.2 mask
255.255.255.0 gateway
192.168.50.1 vlan 8
huawei(config-if-gpon-0/3)#quit
```

Step 3 Configure the in-band management service port.

Set the management VLAN to 8, GEM port ID to 11, and user VLAN to 8. The OLT does not rate limit the in-band management service port. Therefore, directly use the default traffic profile 6.

```
huawei(config)#service-port vlan 8 gpon 0/3/1 ont 1 gemport 11 multi-service
user-vlan 8 rx-cttr 6 tx-cttr 6
```

Step 4 Confirm that the connection between the management service ports on the OLT and ONU is reachable.

- Run the **ping *ONU ip*** command on the OLT to verify the connectivity between the OLT and ONU. If the OLT receives ICMP ECHO-REPLY packets from the ONU, the connection is reachable.
- When the connection is reachable, you can remote log in to the ONU from the OLT and configure the ONU.

----End

14.4.3.5 Configuring OLT QinQ VLANs and Service Ports

This topic describes how to configure QinQ VLANs and service ports to enable various packets received from base stations to be forwarded based on specified policies.

Prerequisites

The MAN equipment (for example, CX600) interconnected with the OLT must support the QinQ VLAN encapsulation mode and be able to terminate QinQ VLANs.

Context

For details on VLAN planning, see **14.2.2 Principle of VLAN Data Plan**. VLAN translation policies for the Ethernet base station access service are shown in **Figure 14-17**.

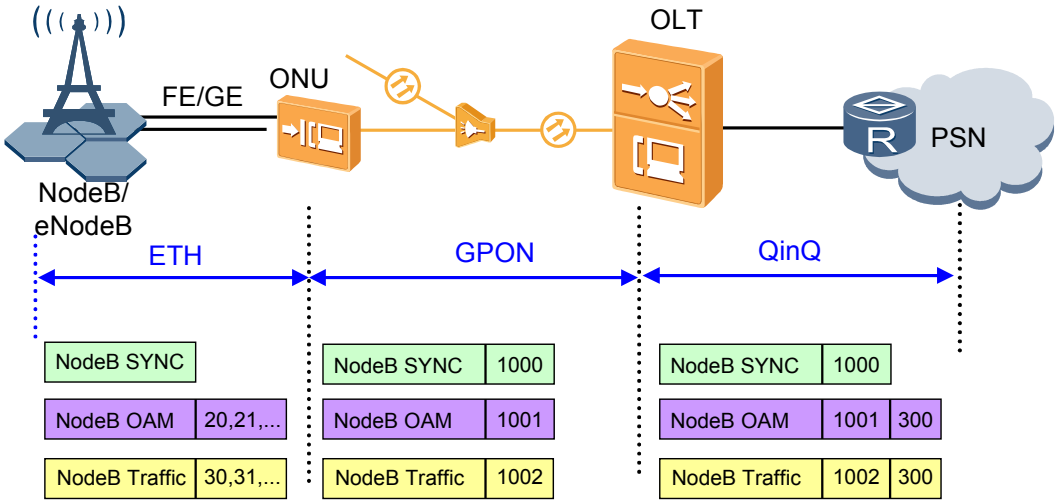
- Synchronization packets (remark 1) of the base station are untagged. A VLAN tag is added to the packets on the ONU and the OLT transparently transmits the VLAN tag.
- Different management packets of the base station carry different user VLANs (for example, 20, 21, ... in the following figure). The user VLANs are translated to CVLAN 1001 on the ONU and then the OLT adds the outer VLAN 300 to the packets before transmitting them upstream.
- Different voice and data packets of the base station carry different user VLANs (for example, 30, 31, ... in the following figure). The user VLANs are translated to CVLAN 1002 on the ONU and then the OLT adds the outer VLAN 300 to the packets before transmitting them upstream.

Copyright © Huawei Technologies Co., Ltd.

In this manner, only two VLANs are required on the MAN for the base station access service, which significantly reduces the number of VLANs.

Remark 1: In this example, the base station supports the clock over IP mode and is synchronized with the IP clock server using the NTP protocol.

Figure 14-17 VLAN translation for Ethernet base station access service



Data Plan

Configuration Item	Data
SVLAN	VLAN for synchronization service of base stations: 1000 VLAN for voice and data services of base stations: 300
CVLAN (upstream VALN of the ONU)	VLAN for base station access service: ● VLAN for synchronization service: 1000 ● VLAN for OAM service: 1001 ● VLAN for voice and data services: 1002
Traffic profile	OAM service and synchronization service of base stations: ● ID: 10 ● CIR: OFF ● Ppriority source: user-cos, default priority: 7 ● Priority policy: tag-in-package Voice and data services of base stations: ● ID: 11 ● CIR: 20 Mbit/s ● Priority source: user-inner-cos, default priority: 7 ● Priority policy: tag-in-package

Copyright © Huawei Technologies Co., Ltd.

Configuration Item	Data
ONT ID	1
PON port	PON port: 0/3/1

Procedure

Step 1 Configure QinQ VLANs.

Add two VLANs 1000 and 300 on the OLT, set attributes of the two VLANs to QinQ, and add the upstream port to the two VLANs.

```
huawei(config)#vlan 1000 smart
huawei(config)#vlan attrib 1000 q-in-q
huawei(config)#port vlan 1000 0/19 0
huawei(config)#vlan 300 smart
huawei(config)#vlan attrib 300 q-in-q
huawei(config)#port vlan 300 0/19 0
```

Step 2 Configure traffic profiles.

- Add a traffic profile 10 and do not limit rates. Packets transmitted upstream use the priority (7 by default) copied from the user VLAN. Packets transmitted downstream use the priority carried by themselves.
- Add a traffic profile 11 and set the assured rate to 20 Mbit/s. Packets transmitted upstream use the priority (7 by default) copied from the inner VLAN. Packets transmitted downstream use the priority carried by themselves.

```
huawei(config)#traffic table ip index 10 cir off priority user-cos 7 priority-policy tag-in-package
huawei(config)#traffic table ip index 11 cir 20480 priority user-inner-cos 7 priority-policy tag-in-package
```

Step 3 Configure service ports.

Configure service ports for the synchronization service, OAM service, and voice and data services of base stations.

```
huawei(config)#service-port vlan 1000 gpon 0/3/1 ont 1 gemport 12 multi-service user-vlan
 1000 tag-transform transparent rx-cttr 10 tx-cttr 10  //Synchronization service port
huawei(config)#service-port vlan 300 gpon 0/3/1 ont 1 gemport 13 multi-service user-vlan
 1001 tag-transform default rx-cttr 10 tx-cttr 10  //OAM service port
huawei(config)#service-port vlan 300 gpon 0/3/1 ont 1 gemport 14 multi-service user-vlan
 1002 tag-transform default rx-cttr 11 tx-cttr 11 //Voice and data service port
```

----End

14.4.3.6 Configuring Ethernet Access Service Ports on ONUs

Add a service port on an ONU and configure an upstream VLAN to make the ONU-to-user service flows available and create an ONU-to-OLT upstream data channel.

Copyright © Huawei Technologies Co., Ltd.

Data Planning

Configuration Item	Data
Port	Upstream port: 0/0/1 Service port: 0/3/1
SVLAN (upstream VLAN of the ONU)	VLAN for base station access service: ● VLAN for synchronization service: 1000 ● VLAN for OAM service: 1001 ● VLAN for voice and data services: 1002
User VLAN (original VLAN of packets from base stations)	● Synchronization service of base stations: untagged ● VLAN for OAM service of base stations: 20 ● VLAN for voice and data services of base stations: 30
Traffic profile	● ID: 10 ● CIR: OFF ● Priority source: user-cos, default priority: 7 ● Priority policy: tag-in-package

Procedure

Step 1 Create SVLANs and add an upstream port to the VLANs.

Create VLANs 1000, 1001, and 1002.

```
huawei(config)#vlan 1000-1002 smart
huawei(config)#port vlan 1000 0/0 1
huawei(config)#port vlan 1001 0/0 1
huawei(config)#port vlan 1002 0/0 1
```

Step 2 Configure a traffic profile.

Add a traffic profile 10 and do not limit rates. Packets transmitted upstream use the priority (7 by default) copied from the user VLAN. Packets transmitted downstream use the priority carried by themselves.

```
huawei(config)#traffic table ip index 10 cir off priority user-cos 7 priority-policy tag-in-package
```

Step 3 Configure Ethernet access service ports.

Configure service ports for the synchronization service, OAM service, and voice and data services of base stations. According to **14.2.2 Principle of VLAN Data Plan**, ONUs translate user VLANs to a specified CVLAN.

```
huawei(config)#service-port vlan 1000 eth 0/3/1 multi-service user-vlan
 untagged rx-cttr 10 tx-cttr 10  //Syncronization service port
huawei(config)#service-port vlan 1001 eth 0/3/1 multi-service user-vlan
 20 rx-cttr 10 tx-cttr 10  //OAM service port
huawei(config)#service-port vlan 1002 eth 0/3/1 multi-service user-vlan
 30 rx-cttr 10 tx-cttr 10 //Voice and data service port
```


Copyright © Huawei Technologies Co., Ltd.

NOTE

Packets from different base stations may carry different user VLANs. Ensure that user VLANs are consistent with the actual ones during configuration.

----End

14.4.3.7 Configuring Clock Synchronization

In this scenario, the synchronous Ethernet clock can be used to achieve network-wide clock synchronization.

Prerequisites

- The clock daughter board CKMC/CKMD of the SCU board must be in position.
- The ethernet upstream board must be GICK/GSCA (GE port) or X2CS (10GE port)/SPUF (need an independent service board slot).
- The upstream MAN PSN of the OLT must feature the capability of Ethernet synchronization.

Context

According to actual requirements, Ethernet base stations support synchronous Ethernet (frequency synchronization) and 1588v2 (time synchronization). This document uses synchronous Ethernet as an example. For details about how to configure 1588v2 time synchronization, see "**14.3.6 Configuring 1588v2 Clock Synchronization**".

Data Plan

Configuration Item	Data
GIU upstream board	Port: 0/19/0
ETH port on the ONU	0/3/1

Procedure

- **Configure a clock on the OLT.**
  1. Add a system clock source.

     Configure the Ethernet line clock input from GIU port 0/19/0 as the system clock 0. Set the priority to 0 (highest priority).

     ```
     huawei(config)#clock source 0 0/19/0
     huawei(config)#clock priority system 0
     ```

  2. Query configurations and the status of the system clock source.

     Run the **display clock source system** command to query configurations and the status of the clock source. Ensure that configurations of the system clock source are correct and the status is **Normal**.

     ```
     huawei(config)#display clock source system
     ```


Copyright © Huawei Technologies Co., Ltd.

```
-------------------------------------------------------------------------
-----
  Index  Board    Source   Clk-type  State       Priority QL
Selected

-------------------------------------------------------------------------
-----
    0    H801GICK 0/19/0    ETH      Normal      0        ---
YES

-------------------------------------------------------------------------
-----
```

Run the **display clock mode** command to query the clock working mode. Ensure that the clock daughter board works in tracing mode.

```
huawei(config)#display clock mode
  Clock manage-mode:Third-mode
  Clock subboard work-mode:Tracing
```

- Configure a clock on the ONU.

  The transmit clock of the port is the system clock by default when base stations are connected to the ONU through ETH ports. The transmit clock cannot be modified. Therefore, you only need to configure the system clock for the ONU.

  1. Configure the PON line clock as the system clock.

     ```
     huawei(config)#clock source 0 0/0/1
     huawei(config)#clock priority system 0
     ```

  2. Query the configuration and status of the system clock source.

     Run the **display clock source** command to query the configuration and status of the system clock source.

     ```
     huawei(config-if-tdm-0/1)#quit
     huawei(config)#display clock source
       ------------------------------------------------------------------
       Index  Type   Source      State         Priority     QL    Selected
       ------------------------------------------------------------------
         0    line   0/0/1       Normal          0          ---      YES
         1    --     -/ -/ -     ---             ---        NO       ---
         2    --     -/ -/ -     ---             ---        NO       ---
         3    --     -/ -/ -     ---             ---        NO       ---
         4    --     -/ -/ -     ---             ---        NO       ---
         5    --     -/ -/ -     ---             ---        NO       ---
         6    --     -/ -/ -     ---             ---        NO       ---
         7    --     -/ -/ -     ---             ---        NO       ---
         8    --     -/ -/ -     ---             ---        NO       ---
         9    --     -/ -/ -     ---             ---        NO       ---
       ------------------------------------------------------------------
     ```

----End

14.4.3.8 Configuring Congestion Control and Security Policies

This topic describes how to configure global priority-based scheduling policies for queues to ensure service reliability and configure global security policies to ensure service security.

Context

Congestion control uses queue scheduling technology to map packets sent from the same port into multiple queues and process packets in each queue based on priority. Congestion control is recommended.

Copyright © Huawei Technologies Co., Ltd.

Security policies cover system security, user security, and service security, which ensure normal running of services.

NOTE

Enable security features based on service types. For details, see **13.2.5 Principle of Security Data Plan**.

Procedure

- Configure queue scheduling.

  Based on **13.2.3 Principle of QoS Data Plan**, all packets use strict priorities for queue scheduling and are mapped to queues based on priorities.

  ```
  huawei(config)#queue-scheduler strict-priority
  huawei(config)#cos-queue-map cos0 0 cos1 1 cos2 2 cos3 3 cos4 4 cos5 5 cos6 6 cos7 7  //System default
  ```

- Configure system security.
  - Enable deny of service (DoS) anti-attack on both the OLT and optical network units (ONUs).
    1. Run the **security anti-dos enable** command to globally enable DoS anti-attack.
    2. Run the **security anti-dos control-packet policy** command to configure a protocol packet processing policy that will be used when a DoS attack occurs.
    3. Run the **security anti-dos control-packet rate** command to configure the threshold for the rate of sending protocol packets to the CPU.
  - Enable IP address anti-attack on both the OLT and ONUs.

    Run the **security anti-ipattack enable** command to enable IP address anti-attack.
- Configure user security.
  - Enable MAC address anti-flapping on both the OLT and ONUs.

    Run the **security anti-macduplicate enable** command to enable MAC address anti-flapping.
  - Enable MAC address anti-spoofing on both the OLT and ONUs.
    1. In global config mode, run the **security anti-macspoofing enable** command to globally enable MAC address anti-spoofing.
    2. Enable MAC address anti-spoofing at VLAN level in global config mode or service profile mode:
       a. In global config mode, run the **security anti-macspoofing vlan** command to enable MAC address anti-spoofing.
       b. Perform the following operations to enable MAC address anti-spoofing in service profile mode:
          a. In global config mode, run the **vlan service-profile** command to create a VLAN service profile.
          b. Run the **security anti-macspoofing enable** command to enable MAC address anti-spoofing at VLAN level.
          c. Run the **commit** command to make the profile configuration take effect.
          d. Run the **quit** command to quit the VLAN service profile mode.
          e. Run the **vlan bind service-profile** command to bind the created VLAN service profile to a VLAN.

Copyright © Huawei Technologies Co., Ltd.

3. (Optional) Run the **security anti-macspoofing max-mac-count** command to set the maximum number of MAC addresses that can be bound to a service flow.
4. (Optional) Run the **security anti-macspoofing exclude** command to configure the types of packets for which MAC address anti-spoofing does not take effect, such as Internet Group Management Protocol (IGMP) packets.

- Enable IP address anti-spoofing on ONUs.

  IP address anti-spoofing can be enabled or disabled at three levels: global, VLAN, and service port levels. This function takes effect only after it is enabled at the three levels. Among the three levels, IP address anti-spoofing is disabled only at the global level by default.

  1. In global config mode, run the **security anti-ipspoofing enable** command to enable IP address anti-spoofing at the global level.
  2. In VLAN service profile mode, run the **security anti-ipspoofing enable** command to enable IP address anti-spoofing at the VLAN level.
  3. Run the **security anti-ipspoofing service-port** *serviceport-id* **enable** command to enable IP address anti-spoofing at the service port level.

----End

14.4.3.9 Configuring Network Protection

This topic describes how to configure end-to-end (E2E) protection schemes for the enterprise private line service which has a high requirement on service reliability.

Context

Reliability covers equipment reliability, upstream networking protection, and downstream networking protection. For details on reliability data planning, see **13.2.6 Principle of Reliability Data Plan**.

- Upstream networking protection includes link aggregation group and protection group. Usually, link aggregation group is configured when the GIU board is used to transmit traffic upstream; protection group is configured when the main control board is used to transmit traffic upstream. The two protection schemes are not configured at the same time.
- Downstream networking protection includes Type B, Type C single homing, and Type C dual homing, which are used to protect service ports. Ports on the same ONU can be configured only with the same protection scheme.

NOTE

This topic describes how to configure five mainstream protection schemes. Select required protection schemes based on the carrier's requirement and actual networking scenario.

Procedure

- Configure a link aggregation group.

  Bind upstream ports 0/19/0 and 0/19/1 together as an aggregation link group. Each member port in the group transmits packets based on source MAC addresses. The working mode is LACP static aggregation.

  ```
  huawei(config)#link-aggregation 0/19 0-1 ingress workmode lacp-static
  ```

- Configure a protection group.

Copyright © Huawei Technologies Co., Ltd.

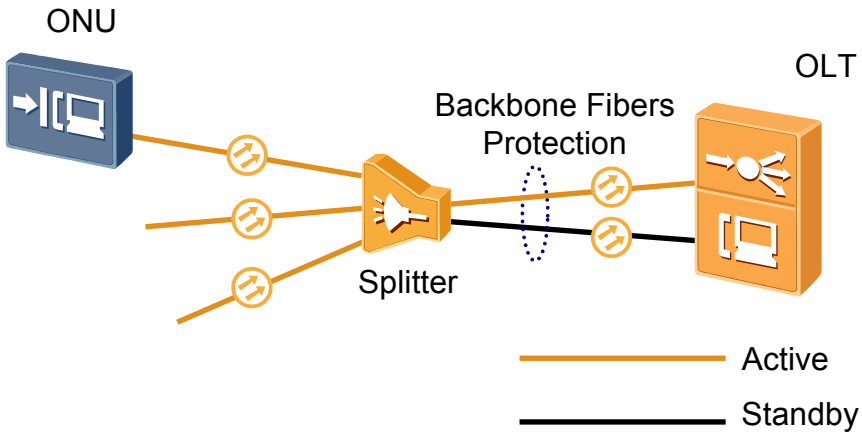
Configure upstream ports 0/19/0 and 0/19/1 on board GIU as a port protection group. Set port 0/19/0 as the working port and port 0/19/1 as the protection port, set the working mode to time delay detection, and enable the protection group.

```
huawei(config-protect)#protect-group first 0/19/0 second 0/19/1 eth workmode timedelay enable
```

- Configure the Type B protection.

  Figure 14-18 shows the Type B protection networking diagram.

  Figure 14-18 Type B protection

  Configure redundancy backup for ports 0/3/1 and 0/3/2 on the same GPON board on OLT. When port 0/3/1 fails, the system can automatically switch to port 0/3/2.

  ```
  huawei(config)#protect-group 0 protect-target gpon-uni-port workmode timedelay
  huawei(protect-group-0)#protect-group member port 0/3/1 role work
  huawei(protect-group-0)#protect-group member port 0/3/2 role protect
  huawei(protect-group-0)#protect-group enable
  ```

  NOTE

  The configurations of services accessed by the ONUs remain the same after the Type B protection is configured. That is, the service configurations are applied only to the working GPON port.

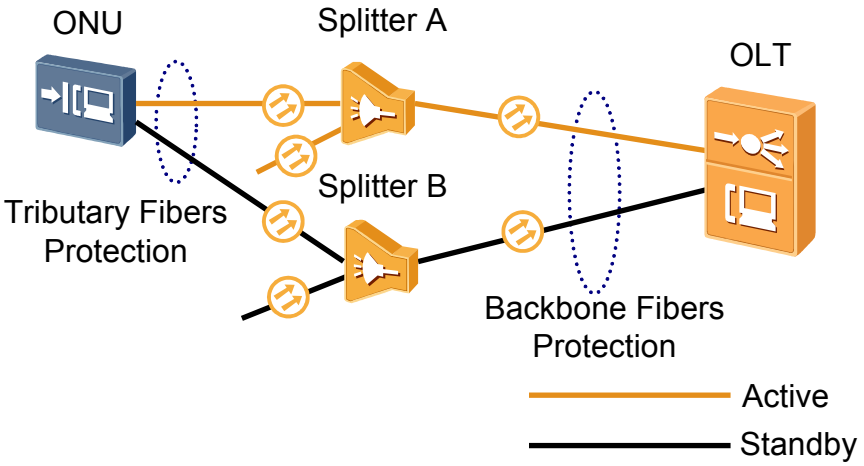
- Configure the Type C single homing protection.

  Figure 14-19 shows networking diagram for the Type C single homing protection. Configure two 1:N optical splitters, one for connecting the working PON ports on the OLT and ONUs, and one for connecting the protection PON ports on the OLT and ONUs. This protection scheme protects both the backbone fibers and tributary fibers.

  The configurations of services accessed by the ONUs remain the same after the Type C single homing protection is configured. That is, the service configurations are applied only to the working PON port on the OLT and working upstream PON ports on the ONUs.

Copyright © Huawei Technologies Co., Ltd.

Figure 14-19 Type C single homing protection



As shown in the preceding figure, Type C single homing protecting is configured for optical fiber links between the OLT and ONU.

- The ports on the GPON service board are 0/3/1 and 0/3/2.
- The link at port 0/3/1 is the working link.
- The link at port 0/3/2 is the protection link.
- The ONU ID is 1.
- The ONU is authenticated by serial number (SN). The SN of the ONU is 32303131B39FD641 and the management mode is SNMP.
- The ID of the line profile bound to the ONU is 10.

```
huawei(config)#interface gpon 0/3
huawei(config-if-gpon-0/3)#ont add 1 1 sn-auth 32303131B39FD641 snmp ont-lineprofile-id 10
huawei(config-if-gpon-0/3)#ont add 2 1 protect-side
huawei(config-if-gpon-0/3)#quit
huawei(config)#protect-group protect-target gpon-uni-ont workmode portstate
huawei(protect-group-1)#protect-group member port 0/3/1 ont 1 role work
huawei(protect-group-1)#protect-group member port 0/3/2 ont 1 role protect
huawei(protect-group-1)#protect-group enable
huawei(protect-group-1)#quit
```

- Configure the Type C dual homing protection.

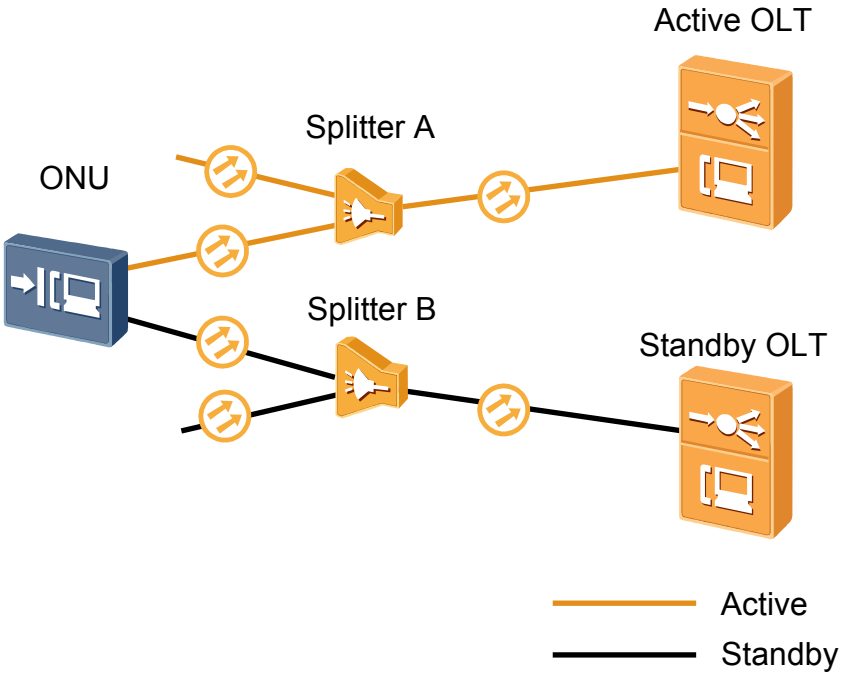
  Figure 14-20 shows the networking diagram for the Type C dual homing protection. Two PON ports on different OLTs, two PON ports on an ONU, two backbone optical fibers, two optical splitters, and two tributary optical fibers are configured to implement this protection. The difference between this protection scheme and the Type C single homing protection scheme is that the ONU needs to be dual homed to two OLTs in this protection scheme.

  The models and versions of main control boards on the active and standby OLTs must be the same. The models and versions of GPON boards on the active and standby OLTs also must be the same. Data on the active OLT cannot be automatically synchronized with that on the standby OLT. Therefore, data synchronization between the active and standby OLTs must be manually ensured.

  This protection scheme can be configured for only the Ethernet QinQ private line service. It does not support TDM services, including Native TDM and SAToP.

Copyright © Huawei Technologies Co., Ltd.

Figure 14-20 Type C dual homing protection



As shown in the preceding figure, Type C dual homing protection is configured for two OLTs (huawei_A and huawei_B).

- huawei_A is the active OLT while huawei_B is the standby OLT.
- The ports on the service boards on both OTLs are 0/3/1.
- The dual homing protection group ID is 1.
- The ONU ID is 1.
- The ONU is authenticated by serial number (SN). The SN of the ONU is 32303131B39FD641 and the management mode is SNMP.
- The ID of the line profile bound to the ONU is 10.

```
Configurations on the active OLT huawei_A:
huawei_A(config)#interface gpon 0/3
huawei_A(config-if-gpon-0/3)#ont add 1 1 sn-auth 32303131B39FD641 snmp ont-
lineprofile-id 10
huawei_A(config-if-gpon-0/3)#quit
huawei_A(config)#protect-group 1 protect-target gpon-uni-ont workmode dual-
parenting
huawei_A(protect-group-1)#protect-group member port 0/3/1 ont 1 role work
Configurations on the standby OLT huawei_B:
huawei_B(config)#interface gpon 0/3
huawei_B(config-if-gpon-0/3)#ont add 1 1 sn-auth 32303131B39FD641 snmp ont-
lineprofile-id 10
huawei_B(config-if-gpon-0/3)#quit
huawei_B(config)#protect-group 1 protect-target gpon-uni-ont workmode dual-
parenting
huawei_B(protect-group-1)#protect-group member port 0/3/1 ont 1 role protect
huawei_B(protect-group-1)#protect-group enable
```

----End

Copyright © Huawei Technologies Co., Ltd.

14.4.3.10 Verifying Services

The Ethernet base station access service can be verified by checking the connectivity and alarms of the service.

Prerequisites

The base station access service has been deployed.

Procedure

Step 1 Check connectivity.

1. Check the connectivity between base stations and the IP clock server.

   On base stations, configure management IP addresses and static routes to the IP clock server, and then perform ping operations. In normal cases, the ICMP ECHO-REPLY message can be received from the IP clock server.

2. Check the connectivity between base stations and the OAM server.

   On base stations, configure IP addresses of management channels and static routes to the OAM server, and then perform ping operations. In normal cases, the ICMP ECHO-REPLY message can be received from the OAM server.

3. Check the connectivity between base stations and the RNC.

   On base stations, configure service port IP addresses and static routes to the RNC, and then perform ping operations. In normal cases, the ICMP ECHO-REPLY message can be received from the RNC.

Step 2 Check alarms.

Check logs on base stations. Verify that no alarms are generated within 24 hours.

----End

14.4.4 Symmetrical TDM PWE3 Access for OLTs on Both Sides

Two OLTs are symmetrically connected to the packet switched network (PSN). Signals of enterprise or base transceiver station (BTS) private line services are transmitted to an ONU through an E1 port, and then the ONU sends the signals to the OLT through GPON lines. The OLT, functioning as a superstratum provider edge (SPE), is connected to its peer OLT through TDM PWE3. This enables the PSN network to carry traditional circuit switched (CS) services.

14.4.4.1 Service Requirements and Application Scenario

Service Requirements

Enhancing O&M capability: The MxU configurations can be performed on the OLT, which simplifies the configuration process.

Minimizing network construction costs: Only 1 SPUB board is required for an OLT.

Allowing TDM services to traverse the packet switched network (PSN): TDM services are deployed independently.

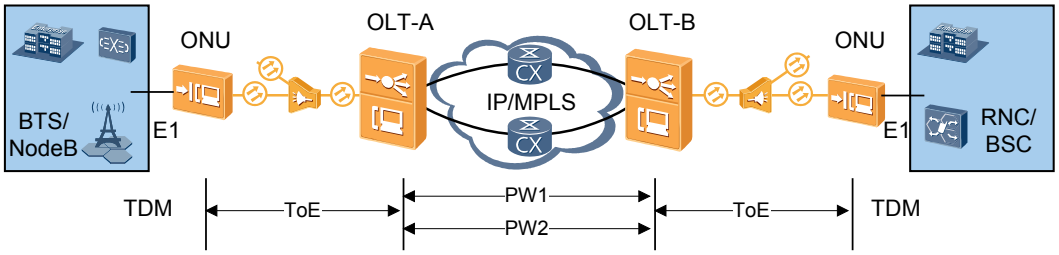
Copyright © Huawei Technologies Co., Ltd.

Application Scenario

As shown in **Figure 14-21**, OLT-A and OLT-B are symmetrically deployed on both sides of the PSN network. Both OLT-A and OLT-B are connected to ONUs through GPON lines. Enterprise or base transceiver station (BTS) private line services are transmitted to the ONUs through E1 ports. Proprietary TOE channels between the ONUs and OLTs are used to encapsulate the packets of TDM services. Symmetrical TDM PWs are created between the 2 OLTs to provide cross-PSN-network access and backhaul for enterprise or BTS private line services.

The model of the ONU supporting this solution is MA5698, MA5898, MA5616.

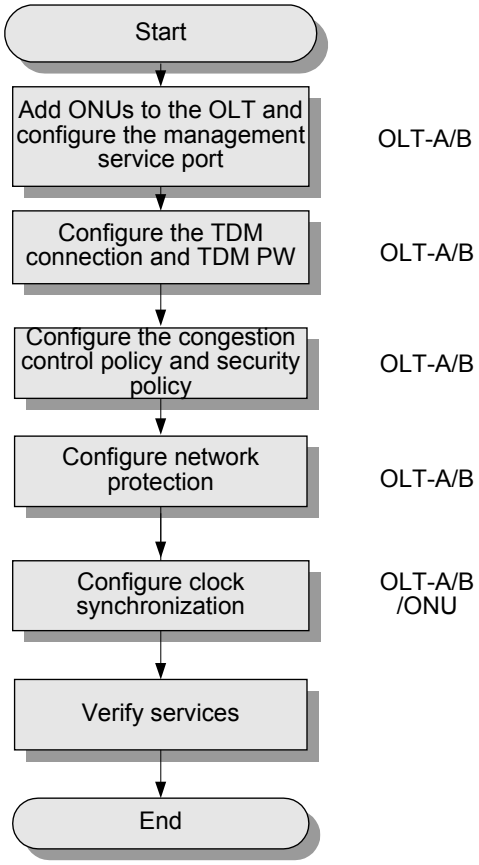
Figure 14-21 Example network of symmetrical GPON TDM PWE3 access



14.4.4.2 Configuration Procedure

The following figure shows the procedure of symmetrically configuring TDM PWE3 access for OLTs on both sides of the packet switched network (PSN). Because the 2 OLTs are symmetrically deployed, the configuration steps on the 2 OLT are the same.

Copyright © Huawei Technologies Co., Ltd.



14.4.4.3 Adding ONUs to the OLT and Configuring the Management Service Port

Related configurations can be performed for ONUs only after the ONUs are successfully added to the OLT. After the inband management service port is created and available, you can log in to the ONUs from the OLT to configure the ONUs.

Context

- When an ONU is added, related profiles need to be bound to the ONU, including the dynamic bandwidth allocation (DBA) profile, line profile, and alarm profile.
- An ONU can be added in two modes: adding an ONU offline and confirming an ONU online. Select either mode as required.

Copyright © Huawei Technologies Co., Ltd.

Data Plan

Table 14-6 Key data plan

Item	Data
DBA profile	DBA profile for management services: system default profile 1 DBA profile for private line services: ● Profile ID: 21 ● Profile type: fixed bandwidth and minimum delay mode ● DBA bandwidth: 28928 kbit/s (assume that 4 E1 private lines are connected to 1 ONU and each E1 private line is configured with a bandwidth of 7232 kbit/s)
Line profile	Profile ID: 11 T-CONT 1 is used for private line services and T-CONT 2 for management services. GEM port ID for management services: 11 GEM port ID for private line services: 13
Networking data	PON port: 0/3/1 ONU parameters: ● ONU ID: 1 ● SN: 32303131B39FD641
Management VLAN and management IP address	On the OLT: Management VLAN ID: 8 Management VLAN type: smart VLAN Inband management IP address: 192.168.50.1/24 On the ONU: Management VLAN ID: 8 Management VLAN type: smart VLAN Inband management IP address: 192.168.50.2/24

Procedure

Step 1 Configure GPON ONU profiles.

1. Configure the DBA profile for private line services, enable bandwidth compensation, and set the DBA bandwidth allocation mode of the GPON port to **min-loop-delay**.

```
huawei(config)#dba-profile add profile-id 21 type1 fix 28928
bandwidth_compensate yes
huawei(config)#interface gpon 0/3
huawei(config-if-gpon-0/3)#port dba bandwidth-assignment-mode 1 min-loop-delay
huawei(config-if-gpon-0/3)#quit
```

2. Configure the ONU line profile.

```
huawei(config)#ont-lineprofile gpon profile-id 11
huawei(config-gpon-lineprofile-11)#tcont 1 dba-profile-id 21  //Bind DBA
```


Copyright © Huawei Technologies Co., Ltd.

```
profile 21 to T-CONT 1.
huawei(config-gpon-lineprofile-11)#tcont 2 dba-profile-id 1  //Bind DBA
profile 1 to T-CONT 2.
huawei(config-gpon-lineprofile-11)#gem add 11 eth tcont 2
huawei(config-gpon-lineprofile-11)#gem add 13 tdm tcont 1 //Add GEM port 13 to
T-CONT 1.
huawei(config-gpon-lineprofile-11)#gem mapping 11 0 vlan 8
huawei(config-gpon-lineprofile-11)#gem mapping 13 1 tdm-vcl //Map GEM port 13
to the TDM connection.
huawei(config-gpon-lineprofile-11)#commit
huawei(config-gpon-lineprofile-11)#quit
```

3. (Optional) Configure the alarm profile.
   - The ID of the default GPON alarm profile is 1. The thresholds for all the alarm parameters in the default alarm profile are 0, which indicates that no alarm is generated.
   - In this example, the default alarm profile is used, and therefore the configuration of the alarm profile is not required.

Step 2 Add an ONU to the OLT.

1. Add ONU 1 offline.

```
huawei(config)#interface gpon 0/3
huawei(config-if-gpon-0/3)#ont add 1 ontid 1 sn-auth 32303131B39FD641
snmp ont-lineprofile-id 11
```

2. (Optional) Bind the alarm profile to ONU 1.

   By default, alarm profile 1 is automatically bound to the ONU. You need to manually bind a non-default alarm profile to the ONU only when the default one does not meet the requirement.

   In this example, default alarm profile 1 is used, and therefore the configuration of the alarm profile is not required.

Step 3 Check the ONU status.

After the ONU is added, run the **display ont info** command to query the status of the ONU. Ensure that **Config flag** of the ONU is **active**, **Run State** is **online**, and **Config state** is **normal**.

To query the status of ONU 1, do as follows:

```
huawei(config-if-gpon-0/3)#display ont info 1 1
  ------------------------------------------------------------------------
  F/S/P                : 0/3/1
  ONT-ID               : 1
  Control flag         : active    //Indicates that the ONU is
activated.
  Run state            : online    //Indicates that the ONU goes online
normally.
  Config state        : normal    //Indicates that the configuration recovery state
of the ONU is normal.
...//The following command output is omitted.
huawei(config-if-gpon-0/3)#quit
```

Step 4 Configure the inband management VLAN and IP address of the OLT.

Create a VLAN whose ID is 8 as the inband management VLAN of the OLT, set the VLAN priority to 6, and set the IP address of the VLAN interface to 192.168.50.1/24.

```
huawei(config)#vlan 8 smart
huawei(config)#vlan priority 8 6
huawei(config)#port vlan 8 0/19 0
huawei(config)#interface vlanif 8
```


Copyright © Huawei Technologies Co., Ltd.

```
huawei(config-if-vlanif8)#ip address 192.168.50.1 24
huawei(config-if-vlanif8)#quit
```

Step 5 Configure the inband management VLAN and IP address of the ONU.

```
huawei(config)#interface gpon 0/3
huawei(config-if-gpon-0/3)#ont ipconfig 1 1 static ip-address 192.168.50.2 mask
255.255.255.0 gateway
192.168.50.1 vlan 8
huawei(config-if-gpon-0/3)#quit
```

Step 6 Configure an inband management service port.

The management VLAN is VLAN 8, the GEM port ID is 11, and user VLAN is VLAN 8. The OLT does not limit the rate of inband management services. Therefore, you can directly bind default traffic profile 6 to the inband management service port.

```
huawei(config)#service-port vlan 8 gpon 0/3/1 ont 1 gemport 11 multi-service
user-vlan 8 rx-cttr 6 tx-cttr 6
```

Step 7 Check whether the management service port between the OLT and the ONU is available.

- Run the **ping *ONU ip*** command on the OLT to check the connectivity between the OLT and the ONU. If the ICMP ECHO-REPLY packets from the ONU are received, the connectivity between the OLT and the ONU is in good condition.
- If you can remotely log in to the ONU from the OLT to perform configurations for the ONU, the management service port between the OLT and the ONU is available.

----End

Follow-up Procedure

When **Config state** is **failed**, **Run state** is **offline**, or **Match state** is **mismatch**:

- If **Control flag** is **deactive**, run the **ont active** command in GPON mode to activate the ONU.
- If **Run state** is **offline**, a physical line may be broken or the optical module may be damaged. Check the line and the optical module.
- If **Config state** is **failed**, the configured ONU capability exceeds the actual ONU capability. In this case, run the **display ont failed-configuration** command in the diagnose mode to check the failed configuration item and the failure cause. Then, rectify the fault accordingly.
- If the ONU does not match, that is, **Match state** is **mismatch**, the port types and number of ports undermatch the actual port types and number of ports supported by the ONU. In this case, run the **display ont capability** command to query the actual capability of the ONU, and then select one of the following modes to modify the ONU configuration:
  - Create a proper ONU profile according to the actual capability of the ONU, and then run the **ont modify** command to modify the configuration data of the ONU.
  - Modify the ONU profile according to the actual capability of the ONU and save the modification. Then, the ONU automatically recovers the configuration successfully.

14.4.4.4 Configuring the TDM Connection and TDM PW

A TDM connection between the OLT and ONU is created and bound to the PW, so that TDM PWE3 services can be transmitted between two OLTs.

Copyright © Huawei Technologies Co., Ltd.

Prerequisites

The SPUB board is in position and functions normally.

Data Plan

When OLTs are symmetrically connected to the packet switched network (PSN), the configuration steps for OLT-A and OLT-B are the same, and only the configuration data varies with the OLTs. The varied configuration data of OLT-A and OLT-B will be separately described in this topic.

Table 14-7 Key data plan

Item	Data
VLAN	1000
ONU E1 port	● Port ID: 0/1/0 ● Port signaling mode: unstructured data transfer (UDT) ● Transmit clock of the port: system clock
IP address	OLT-A: ● IP address of the VLAN interface: 10.0.0.10/24 ● IP address of the loopback interface: 1.1.1.1/32 OLT-B: ● IP address of the VLAN interface: 10.0.0.20/24 ● IP address of the loopback interface: 2.2.2.2/32
PW parameters	The following parameters must be the same on the 2 OLTs. ● PW ID: 1 ● PW type: TDM SAToP E1 ● Control word: enabled ● PW load time: 125 μs ● Size of jitter buffer: 500 μs ● RTP header: enabled

Procedure

Step 1 Configure the TDM connection.

1. Configure the TDM virtual channel link (VCL) on the ONU.

   On GPON port 0/3/1, create the TDM VCL for E1 port 0/1/0 of ONU 0.

   NOTE

   Each E81A board has 8 E1 ports. Port IDs 0 to 7 on board 0/1 correspond to ONT port IDs 1 to 8, port IDs 0 to 7 on board 0/2 correspond to ONT port IDs 9 to 16, and so forth.

   ```
   huawei(config-if-gpon-0/3)ont tdm-vcl 1 0 tdm-vcl-id 0 satop 1
   huawei(config-if-gpon-0/3)quit
   ```


Copyright © Huawei Technologies Co., Ltd.

2. Configure the TDM connection on the OLT.

```
huawei(config)tdm-connect connectid 0 tdm pwe3-uplink gpon 0/3/11 ontid 1
gemportIndex 13 tdm-vcl 0
```

Step 2 Configure the basic functions of multiprotocol label switching (MPLS).

1. Create VLAN 1000, add the upstream port into VLAN 1000, and configure the IP address of VLAN interface 1000.

```
huawei(config)#vlan 1000 smart
huawei(config)#port vlan 1000 0/19 0
huawei(config)#interface vlanif 1000
huawei(config-if-vlanif1000)#ip address 10.0.0.10 24
```

2. Configure the IP address of the loopback interface and MPLS LSR ID.

```
huawei(config)#interface loopback 0
huawei(config-if-loopback0)#ip address 1.1.1.1 32
huawei(config)#mpls lsr-id 1.1.1.1
```

3. Enable MPLS, MPLS L2VPN, and MPLS LDP globally, and then enable MPLS and MPLS LDP for the VLAN interface.

```
huawei(config)#mpls
Info: Mpls starting, please wait... OK!
huawei(config-mpls)#quit
huawei(config)#mpls l2vpn
huawei(config)#mpls ldp
huawei(config)#mpls vlan 1000
huawei(config)#interface vlanif 1000
huawei(config-if-vlanif1000)#mpls
huawei(config-if-vlanif1000)#mpls ldp
```

4. Configure a static route to the peer OLT.

   Configure a static route from OLT-A to OLT-B.

```
huawei(config)#ip route-static 2.2.2.2 32 10.0.0.20
```

   Configure a static route from OLT-B to OLT-A.

```
huawei(config)#ip route-static 1.1.1.1 32 10.0.0.10
```

   After the static routes are configured successfully, ping the VLAN interface or LSR ID of the peer OLT from one OLT. Normally, the ICMP ECHO-REPLY packets from the peer OLT can be received.

Step 3 Configure the MPLS PW.

PW parameter **peer-address** (configured on the 2 OLTs) is set to the LSR ID of the peer OLT, and other PW parameters must be set identically on the 2 OLTs.

```
huawei(config)#pw-para 1
huawei(config-pw-para-1)#peer-address 1.1.1.1  //Set the peer address to the LSR ID
of the peer OLT.
huawei(config-pw-para-1)#pw-type tdm satop e1  //The PW type must be the same as
the attribute of the E1 port on the ONU.
                                               //Configure the SAToP encapsulation,
and set the E1 port signaling mode to UDT.
huawei(config-pw-para-1)#control-word
huawei(config-pw-para-1)#tdm-load-time satop e1 loadtime 125
huawei(config-pw-para-1)#jitter-buffer buffer-size 500
huawei(config-pw-para-1)#rtp-header encap payload-type 0 sn 0 ssrc rcv 0 tx 0
huawei(config-pw-para-1)#quit
```

Step 4 Dynamically bind PW 1 to the TDM connection.

```
huawei(config)#pw-ac-binding tdm 0 pw 1
```

Step 5 Configure the attributes of the E1 port on the ONU.

Copyright © Huawei Technologies Co., Ltd.

Log in to the ONU from the OLT, and then configure the port signaling mode of E1 port 0/1/0 to **UDT** and the transmit clock to **system**.

```
huawei(config)#interface tdm 0/1
huawei(config-if-tdm-0/1)#port 0 udt system
huawei(config-if-tdm-0/1)#quit
```

----End

Follow-up Procedure

After all the configurations are performed successfully, the related information about the CESoP connection can be queried by running the **display cesop-connect** command on the ONU.

```
huawei(config)#display cesop-connect all
  ------------------------------------------------------------------------------
  ID     PORT VCL ENCAP      REMOTEMAC         REMOTEIP LOCALUDP   REMOTEUDP VLAN
               ID  TYPE                              /RXPWLABEL  /TXPWLABEL
  ------------------------------------------------------------------------------
  0    0/1 /0   0  MPLS e024-7f98-a21b               -    9343        8192  TOE
  ------------------------------------------------------------------------------
  Total: 1
```

14.4.4.5 Configuring Clock Synchronization

In this scenario, network-wide clock synchronization is implemented through synchronous Ethernet clocks.

Prerequisites

- The clock daughter board CKMC/CKMD of the SCU control board is in position.
- The Ethernet upstream board is the GICK/GSCA (GE port) or X2CS/SPUF (10GE port) board.
- The upstream MAN PSN of the OLT supports Synchronous Ethernet.

Data Plan

Item	Data
Ethernet upstream board	Port: 0/19/0 **NOTE** The SPUF board exclusively occupies a service slot. This topic uses the GIU upstream board as an example.

Procedure

- **Configure the OLT-side clock.**
  1. Configure a system clock source.

     Use the Ethernet line clock input from GIU port 0/19/0 as the system clock. Set the index of the system clock to **0** and priority to **0** (highest priority).

     ```
     huawei(config)#clock source 0 0/19/0
     huawei(config)#clock priority system 0
     ```

  2. Query the configurations and status of the system clock source.

Copyright © Huawei Technologies Co., Ltd.

Run the **display clock source system** command to query the configurations and status of the clock source. Ensure that the configurations of the system clock source are correct and the status of the system clock source is **Normal**.

```
huawei(config)#display clock source system

-------------------------------------------------------------------------
-----
  Index  Board    Source   Clk-type  State       Priority QL
Selected

-------------------------------------------------------------------------
-----
    0    H801GICK 0/19/0    ETH      Normal      0        ---
YES

-------------------------------------------------------------------------
-----
```

Run the **display clock mode** command to query the working mode of the clock. Ensure that the working mode of the clock daughter board is **Tracing**.

```
huawei(config)#display clock mode
  Clock manage-mode:Third-mode
  Clock subboard work-mode:Tracing
```

- **Configure the ONU-side clock.**
  1. Configure the PON line clock as the system clock.

     ```
     huawei(config)#clock source 0 0/0/1
     huawei(config)#clock priority system 0
     ```

  2. Query the configuration and status of the system clock source.

     Run the **display clock source** command to query the configuration and status of the system clock source.

     ```
     huawei(config-if-tdm-0/1)#quit
     huawei(config)#display clock source
       ------------------------------------------------------------------------
       Index  Type   Source      State          Priority     QL    Selected
       ------------------------------------------------------------------------
         0    line   0/0/1       Normal           0          ---       YES
         1    --     -/ -/ -     ---              ---        NO        ---
         2    --     -/ -/ -     ---              ---        NO        ---
         3    --     -/ -/ -     ---              ---        NO        ---
         4    --     -/ -/ -     ---              ---        NO        ---
         5    --     -/ -/ -     ---              ---        NO        ---
         6    --     -/ -/ -     ---              ---        NO        ---
         7    --     -/ -/ -     ---              ---        NO        ---
         8    --     -/ -/ -     ---              ---        NO        ---
         9    --     -/ -/ -     ---              ---        NO        ---
       ------------------------------------------------------------------------
     ```

----End

14.4.4.6 Configuring Congestion Control and Security Policies

This topic describes how to configure global priority-based scheduling policies for queues to ensure service reliability and configure global security policies to ensure service security.

Context

Congestion control uses queue scheduling technology to map packets sent from the same port into multiple queues and process packets in each queue based on priority. Congestion control is recommended.

Copyright © Huawei Technologies Co., Ltd.

Security policies cover system security, user security, and service security, which ensure normal running of services.

NOTE

Enable security features based on service types. For details, see **13.2.5 Principle of Security Data Plan**.

Procedure

- Configure queue scheduling.

  Based on **13.2.3 Principle of QoS Data Plan**, all packets use strict priorities for queue scheduling and are mapped to queues based on priorities.

  ```
  huawei(config)#queue-scheduler strict-priority
  huawei(config)#cos-queue-map cos0 0 cos1 1 cos2 2 cos3 3 cos4 4 cos5 5 cos6 6 cos7 7  //System default
  ```

- Configure system security.
  - Enable deny of service (DoS) anti-attack on both the OLT and optical network units (ONUs).
    1. Run the **security anti-dos enable** command to globally enable DoS anti-attack.
    2. Run the **security anti-dos control-packet policy** command to configure a protocol packet processing policy that will be used when a DoS attack occurs.
    3. Run the **security anti-dos control-packet rate** command to configure the threshold for the rate of sending protocol packets to the CPU.
  - Enable IP address anti-attack on both the OLT and ONUs.

    Run the **security anti-ipattack enable** command to enable IP address anti-attack.
- Configure user security.
  - Enable MAC address anti-flapping on both the OLT and ONUs.

    Run the **security anti-macduplicate enable** command to enable MAC address anti-flapping.
  - Enable MAC address anti-spoofing on both the OLT and ONUs.
    1. In global config mode, run the **security anti-macspoofing enable** command to globally enable MAC address anti-spoofing.
    2. Enable MAC address anti-spoofing at VLAN level in global config mode or service profile mode:
       a. In global config mode, run the **security anti-macspoofing vlan** command to enable MAC address anti-spoofing.
       b. Perform the following operations to enable MAC address anti-spoofing in service profile mode:
          a. In global config mode, run the **vlan service-profile** command to create a VLAN service profile.
          b. Run the **security anti-macspoofing enable** command to enable MAC address anti-spoofing at VLAN level.
          c. Run the **commit** command to make the profile configuration take effect.
          d. Run the **quit** command to quit the VLAN service profile mode.
          e. Run the **vlan bind service-profile** command to bind the created VLAN service profile to a VLAN.

Copyright © Huawei Technologies Co., Ltd.

3. (Optional) Run the **security anti-macspoofing max-mac-count** command to set the maximum number of MAC addresses that can be bound to a service flow.
4. (Optional) Run the **security anti-macspoofing exclude** command to configure the types of packets for which MAC address anti-spoofing does not take effect, such as Internet Group Management Protocol (IGMP) packets.

- Enable IP address anti-spoofing on ONUs.

  IP address anti-spoofing can be enabled or disabled at three levels: global, VLAN, and service port levels. This function takes effect only after it is enabled at the three levels. Among the three levels, IP address anti-spoofing is disabled only at the global level by default.

  1. In global config mode, run the **security anti-ipspoofing enable** command to enable IP address anti-spoofing at the global level.
  2. In VLAN service profile mode, run the **security anti-ipspoofing enable** command to enable IP address anti-spoofing at the VLAN level.
  3. Run the **security anti-ipspoofing service-port** *serviceport-id* **enable** command to enable IP address anti-spoofing at the service port level.

----End

14.4.4.7 Configuring E2E Reliability

This topic describes how to configure end-to-end (E2E) protection schemes for the enterprise private line service which has a high requirement on service reliability.

Context

Reliability covers equipment reliability, upstream networking protection, and downstream networking protection. For details on reliability data planning, see **13.2.6 Principle of Reliability Data Plan**.

- Upstream networking protection includes link aggregation group and protection group. Usually, link aggregation group is configured when the GIU board is used to transmit traffic upstream; protection group is configured when the main control board is used to transmit traffic upstream. The two protection schemes are not configured at the same time.
- Downstream networking protection includes Type B, Type C single homing, and Type C dual homing, which are used to protect service ports. Ports on the same ONU can be configured only with the same protection scheme.

NOTE

This topic describes how to configure five mainstream protection schemes. Select required protection schemes based on the carrier's requirement and actual networking scenario.

Procedure

- Configure a link aggregation group.

  Bind upstream ports 0/19/0 and 0/19/1 together as an aggregation link group. Each member port in the group transmits packets based on source MAC addresses. The working mode is LACP static aggregation.

  ```
  huawei(config)#link-aggregation 0/19 0-1 ingress workmode lacp-static
  ```

- Configure a protection group.

Copyright © Huawei Technologies Co., Ltd.

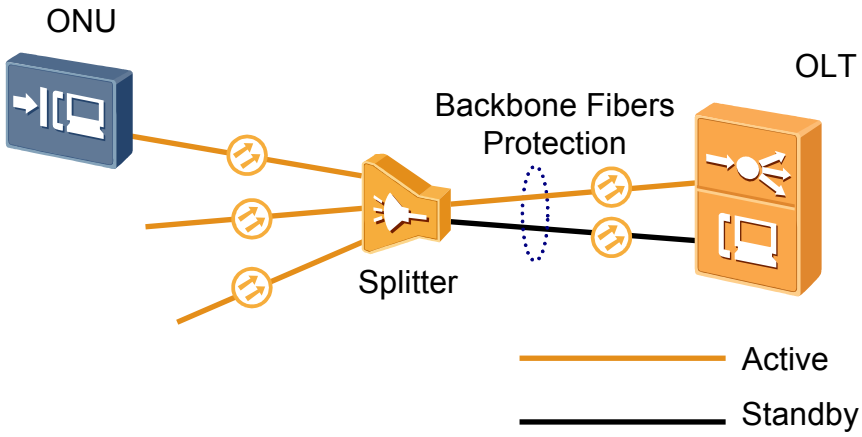
Configure upstream ports 0/19/0 and 0/19/1 on board GIU as a port protection group. Set port 0/19/0 as the working port and port 0/19/1 as the protection port, set the working mode to time delay detection, and enable the protection group.

```
huawei(config-protect)#protect-group first 0/19/0 second 0/19/1 eth workmode timedelay enable
```

- Configure the Type B protection.

  Figure 14-22 shows the Type B protection networking diagram.

  Figure 14-22 Type B protection

  Configure redundancy backup for ports 0/3/1 and 0/3/2 on the same GPON board on OLT. When port 0/3/1 fails, the system can automatically switch to port 0/3/2.

  ```
  huawei(config)#protect-group 0 protect-target gpon-uni-port workmode timedelay
  huawei(protect-group-0)#protect-group member port 0/3/1 role work
  huawei(protect-group-0)#protect-group member port 0/3/2 role protect
  huawei(protect-group-0)#protect-group enable
  ```

  NOTE

  The configurations of services accessed by the ONUs remain the same after the Type B protection is configured. That is, the service configurations are applied only to the working GPON port.

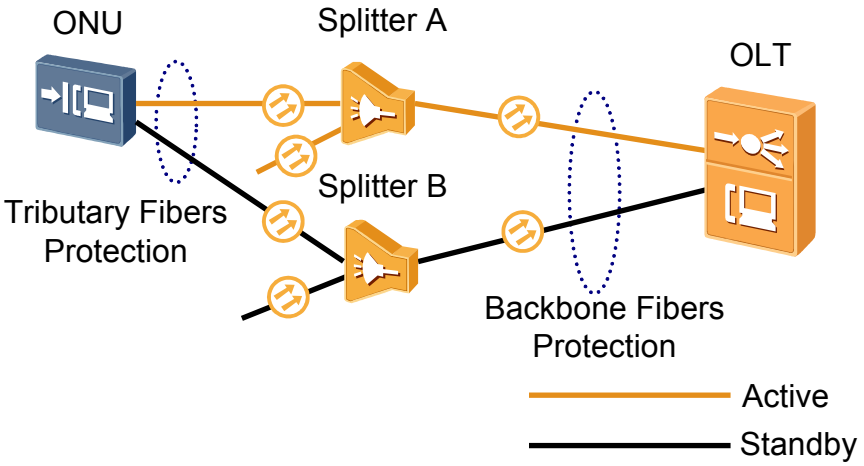
- Configure the Type C single homing protection.

  Figure 14-23 shows networking diagram for the Type C single homing protection. Configure two 1:N optical splitters, one for connecting the working PON ports on the OLT and ONUs, and one for connecting the protection PON ports on the OLT and ONUs. This protection scheme protects both the backbone fibers and tributary fibers.

  The configurations of services accessed by the ONUs remain the same after the Type C single homing protection is configured. That is, the service configurations are applied only to the working PON port on the OLT and working upstream PON ports on the ONUs.

Copyright © Huawei Technologies Co., Ltd.

Figure 14-23 Type C single homing protection



As shown in the preceding figure, Type C single homing protecting is configured for optical fiber links between the OLT and ONU.

- The ports on the GPON service board are 0/3/1 and 0/3/2.
- The link at port 0/3/1 is the working link.
- The link at port 0/3/2 is the protection link.
- The ONU ID is 1.
- The ONU is authenticated by serial number (SN). The SN of the ONU is 32303131B39FD641 and the management mode is SNMP.
- The ID of the line profile bound to the ONU is 10.

```
huawei(config)#interface gpon 0/3
huawei(config-if-gpon-0/3)#ont add 1 1 sn-auth 32303131B39FD641 snmp ont-lineprofile-id 10
huawei(config-if-gpon-0/3)#ont add 2 1 protect-side
huawei(config-if-gpon-0/3)#quit
huawei(config)#protect-group protect-target gpon-uni-ont workmode portstate
huawei(protect-group-1)#protect-group member port 0/3/1 ont 1 role work
huawei(protect-group-1)#protect-group member port 0/3/2 ont 1 role protect
huawei(protect-group-1)#protect-group enable
huawei(protect-group-1)#quit
```

- Configure the Type C dual homing protection.

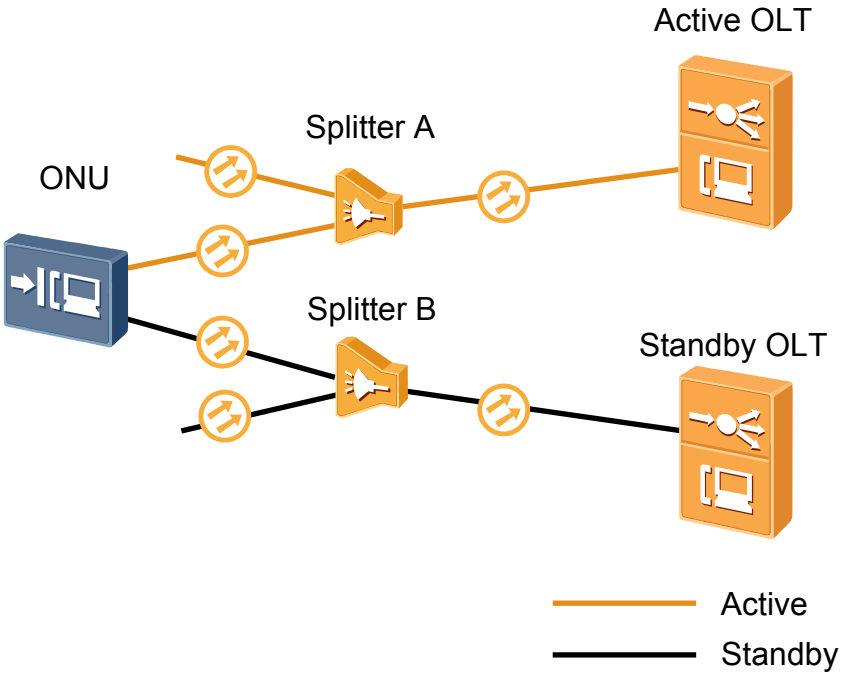
  Figure 14-24 shows the networking diagram for the Type C dual homing protection. Two PON ports on different OLTs, two PON ports on an ONU, two backbone optical fibers, two optical splitters, and two tributary optical fibers are configured to implement this protection. The difference between this protection scheme and the Type C single homing protection scheme is that the ONU needs to be dual homed to two OLTs in this protection scheme.

  The models and versions of main control boards on the active and standby OLTs must be the same. The models and versions of GPON boards on the active and standby OLTs also must be the same. Data on the active OLT cannot be automatically synchronized with that on the standby OLT. Therefore, data synchronization between the active and standby OLTs must be manually ensured.

  This protection scheme can be configured for only the Ethernet QinQ private line service. It does not support TDM services, including Native TDM and SAToP.

Copyright © Huawei Technologies Co., Ltd.

Figure 14-24 Type C dual homing protection



As shown in the preceding figure, Type C dual homing protection is configured for two OLTs (huawei_A and huawei_B).

- huawei_A is the active OLT while huawei_B is the standby OLT.
- The ports on the service boards on both OTLs are 0/3/1.
- The dual homing protection group ID is 1.
- The ONU ID is 1.
- The ONU is authenticated by serial number (SN). The SN of the ONU is 32303131B39FD641 and the management mode is SNMP.
- The ID of the line profile bound to the ONU is 10.

```
Configurations on the active OLT huawei_A:
huawei_A(config)#interface gpon 0/3
huawei_A(config-if-gpon-0/3)#ont add 1 1 sn-auth 32303131B39FD641 snmp ont-
lineprofile-id 10
huawei_A(config-if-gpon-0/3)#quit
huawei_A(config)#protect-group 1 protect-target gpon-uni-ont workmode dual-
parenting
huawei_A(protect-group-1)#protect-group member port 0/3/1 ont 1 role work
Configurations on the standby OLT huawei_B:
huawei_B(config)#interface gpon 0/3
huawei_B(config-if-gpon-0/3)#ont add 1 1 sn-auth 32303131B39FD641 snmp ont-
lineprofile-id 10
huawei_B(config-if-gpon-0/3)#quit
huawei_B(config)#protect-group 1 protect-target gpon-uni-ont workmode dual-
parenting
huawei_B(protect-group-1)#protect-group member port 0/3/1 ont 1 role protect
huawei_B(protect-group-1)#protect-group enable
```

----End

Copyright © Huawei Technologies Co., Ltd.

14.4.4.8 Verifying Services

Verifying private line services requires a dedicated E1 line test instrument.

Prerequisites

The configuration of private line services has been completed.

Context

Because E1 access is applied to both sides of the packet switched network (PSN), an E1 line test instrument can be used to verify services. The E1 line test instrument is connected to the E1 port of the device on one side of the network after the port loopback or hardware loopback is configured on the E1 port of the device on the other side of the network.

Procedure

Step 1 Configure a local loopback on the E1 port.

If the E1 port of the ONU is used to provide access for the private line services, the configurations are as follows:

```
huawei(config)#interface tdm 0/1
huawei(config-if-tdm-0/1)#loopback 0 local
  This operation will interrupt the service, continue? (y/n)[n]:y
```

If the E1 port of the EDTB board is used to provide access for the private line services, the configurations are as follows:

```
huawei(config)#interface edt 0/2
huawei(config-if-edt-0/2)#loopback 0 local
```

Step 2 Use the E1 line test instrument to send packets.

NOTE

Ensure the synchronization between clocks. It is recommended that the E1 line test instrument should use the self-generated clock, the OLT should trace the clock of the E1 line test instrument, and the ONU should trace the clock of the OLT.

The test duration must be equal to or longer than 12 hours. No alarm information is displayed on the test instrument, and the bit error rate (BER) must be lower than 1E-9.

----End

Follow-up Procedure

You can collect the packet statistics to check whether the CESoP and TDM connections are normal.

- Collect the statistics of packets sent and received by the CESoP connection on the ONU.

```
huawei(config)#display cesop-connect statistics 0
  ------------------------------------------------------
  CONNECTID : 0
  ------------------------------------------------------
  Lost Packet Count:                0
  Received Packet Count:            58733
  Transmitted Packet Count:         58732
  Overflow Jitter Buffer Times:     0
  Underflow Jitter Buffer Times:    0
  Received Abnormal Packet Count:   0
```


Copyright © Huawei Technologies Co., Ltd.

```
  Received Sn-error Packet Count:   0
  Received Ssrc-error Packet Count: 0
  ----------------------------------------------------
```

In the command output, the number of received packets must be the same as that of sent packets.

- Collect the statistics of packets sent and received by the TDM connection on the OLT.

```
huawei(config)#display tdm-connect statistics 0
-------------------------------------------------------------
   Statistics on ONU side:
   Discarded Packets                                : 0
   Received Packets                                 : 132252
   Transmitted Packets                              : 132253
   Received Error CESoP Packets                     : 0
   Received SN Error CESoP Packets                  : 0
   Received SSRC Error CESoP Packets                : 0
  -------------------------------------------------------------
```

In the command output, the number of received packets must be the same as that of sent packets.

14.4.5 GPON Access for the OLT one Side and E1 or SHDSL access for the OLT on the Peer Side

Signals of enterprise or base transceiver station (BTS) private line services are transmitted to an ONU through an E1 port on one side of the packet switched network (PSN), and then transmitted to the OLT through GPON lines. The OLT functions as a superstratum provider edge (SPE) in this scenario. On the other side of the PSN network, signals of enterprise or BTS private line services are transmitted to the OLT through E1 or SHDSL lines. TDM PWE3 is created between the 2 OLTs on both sides of the PSN network to enable the PSN network to carry traditional circuit switched (CS) services.

14.4.5.1 Service Requirements and Application Scenario

Service Requirements

Enhancing O&M capability: The MxU configurations can be performed on the OLT, which simplifies the configuration process.

Minimizing network construction costs: Only 1 SPUB board is required for an OLT.

Allowing TDM services to traverse the packet switched network (PSN): TDM services are deployed independently.

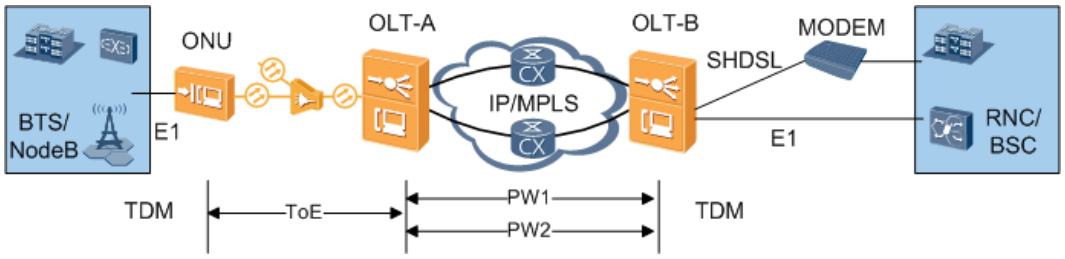
Application Scenario

As shown in **Figure 14-25**, OLT-A and OLT-B are deployed on both sides of the PSN network. OLT-A is connected to an ONU through GPON lines. Enterprise or base transceiver station (BTS) private line services are transmitted to the ONU through an E1 port. A proprietary TOE channel between the ONU and OLT is used to encapsulate the packets of TDM services. Enterprise or BTS private line services are transmitted to OLT-B through E1 or SHDSL lines. TDM PWs are created between the 2 OLTs to provide cross-PSN-network access and backhaul for enterprise or BTS private line services.

The model of the ONU supporting this solution is MA5698, MA5898, MA5616.

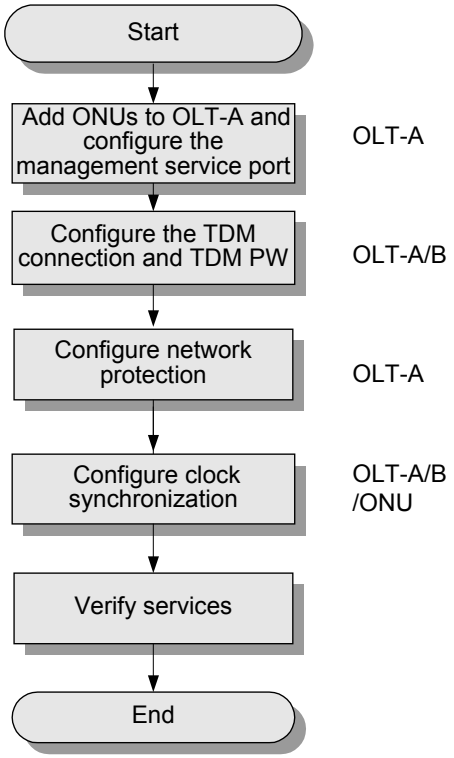
Copyright © Huawei Technologies Co., Ltd.

Figure 14-25 Example network of GPON access on one side and E1 or SHDSL access on the peer side



14.4.5.2 Configuration Procedure

The following figure shows the procedure of configuring GPON access for the OLT on one side and E1 or SHDSL access for the OLT on the peer side of the packet switched network (PSN). The configuration steps on the 2 OLT are the same, but the methods for configuring TDM connections on the 2 OLTs are different.



14.4.5.3 Adding ONUs to OLT-A and Configuring the Management Service Port

Related configurations can be performed for ONUs only after the ONUs are successfully added to OLT-A. After the inband management service port is created and available, you can log in to the ONUs from the OLT to configure the ONUs.

Copyright © Huawei Technologies Co., Ltd.

Context

- When an ONU is added, related profiles need to be bound to the ONU, including the dynamic bandwidth allocation (DBA) profile, line profile, and alarm profile.
- An ONU can be added in two modes: adding an ONU offline and confirming an ONU online. Select either mode as required.

Data Plan

Table 14-8 Key data plan

Item	Data
DBA profile	DBA profile for management services: system default profile 1 DBA profile for private line services: ● Profile ID: 21 ● Profile type: fixed bandwidth and minimum delay mode ● DBA bandwidth: 28928 kbit/s (assume that 4 E1 private lines are connected to 1 ONU and each E1 private line is configured with a bandwidth of 7232 kbit/s)
Line profile	Profile ID: 11 T-CONT 1 is used for private line services and T-CONT 2 for management services. GEM port ID for management services: 11 GEM port ID for private line services: 13
Networking data	PON port: 0/3/1 ONU parameters: ● ONU ID: 1 ● SN: 32303131B39FD641
Management VLAN and management IP address	On the OLT: Management VLAN ID: 8 Management VLAN type: smart VLAN Inband management IP address: 192.168.50.1/24 On the ONU: Management VLAN ID: 8 Management VLAN type: smart VLAN Inband management IP address: 192.168.50.2/24

Procedure

Step 1 Configure GPON ONU profiles.

1. Configure the DBA profile for private line services, enable bandwidth compensation, and set the DBA bandwidth allocation mode of the GPON port to **min-loop-delay**.

Copyright © Huawei Technologies Co., Ltd.

```
huawei(config)#dba-profile add profile-id 21 type1 fix 28928
bandwidth_compensate yes
huawei(config)#interface gpon 0/3
huawei(config-if-gpon-0/3)#port dba bandwidth-assignment-mode 1 min-loop-delay
huawei(config-if-gpon-0/3)#quit
```

2. Configure the ONU line profile.

```
huawei(config)#ont-lineprofile gpon profile-id 11
huawei(config-gpon-lineprofile-11)#tcont 1 dba-profile-id 21  //Bind DBA
profile 21 to T-CONT 1.
huawei(config-gpon-lineprofile-11)#tcont 2 dba-profile-id 1  //Bind DBA
profile 1 to T-CONT 2.
huawei(config-gpon-lineprofile-11)#gem add 11 eth tcont 2
huawei(config-gpon-lineprofile-11)#gem add 13 tdm tcont 1 //Add GEM port 13 to
T-CONT 1.
huawei(config-gpon-lineprofile-11)#gem mapping 11 0 vlan 8
huawei(config-gpon-lineprofile-11)#gem mapping 13 1 tdm-vcl //Map GEM port 13
to the TDM connection.
huawei(config-gpon-lineprofile-11)#commit
huawei(config-gpon-lineprofile-11)#quit
```

3. (Optional) Configure the alarm profile.
   - The ID of the default GPON alarm profile is 1. The thresholds for all the alarm parameters in the default alarm profile are 0, which indicates that no alarm is generated.
   - In this example, the default alarm profile is used, and therefore the configuration of the alarm profile is not required.

Step 2 Add an ONU to the OLT.

1. Add ONU 1 offline.

```
huawei(config)#interface gpon 0/3
huawei(config-if-gpon-0/3)#ont add 1 ontid 1 sn-auth 32303131B39FD641
snmp ont-lineprofile-id 11
```

2. (Optional) Bind the alarm profile to ONU 1.

   By default, alarm profile 1 is automatically bound to the ONU. You need to manually bind a non-default alarm profile to the ONU only when the default one does not meet the requirement.

   In this example, default alarm profile 1 is used, and therefore the configuration of the alarm profile is not required.

Step 3 Check the ONU status.

After the ONU is added, run the **display ont info** command to query the status of the ONU. Ensure that **Config flag** of the ONU is **active**, **Run State** is **online**, and **Config state** is **normal**.

To query the status of ONU 1, do as follows:

```
huawei(config-if-gpon-0/3)#display ont info 1 1
  ------------------------------------------------------------------------
  F/S/P                : 0/3/1
  ONT-ID               : 1
  Control flag         : active    //Indicates that the ONU is
activated.
  Run state            : online    //Indicates that the ONU goes online
normally.
  Config state        : normal    //Indicates that the configuration recovery state
of the ONU is normal.
...//The following command output is omitted.
huawei(config-if-gpon-0/3)#quit
```

Step 4 Configure the inband management VLAN and IP address of the OLT.

Copyright © Huawei Technologies Co., Ltd.

Create a VLAN whose ID is 8 as the inband management VLAN of the OLT, set the VLAN priority to 6, and set the IP address of the VLAN interface to 192.168.50.1/24.

```
huawei(config)#vlan 8 smart
huawei(config)#vlan priority 8 6
huawei(config)#port vlan 8 0/19 0
huawei(config)#interface vlanif 8
huawei(config-if-vlanif8)#ip address 192.168.50.1 24
huawei(config-if-vlanif8)#quit
```

Step 5 Configure the inband management VLAN and IP address of the ONU.

```
huawei(config)#interface gpon 0/3
huawei(config-if-gpon-0/3)#ont ipconfig 1 1 static ip-address 192.168.50.2 mask
255.255.255.0 gateway
192.168.50.1 vlan 8
huawei(config-if-gpon-0/3)#quit
```

Step 6 Configure an inband management service port.

The management VLAN is VLAN 8, the GEM port ID is 11, and user VLAN is VLAN 8. The OLT does not limit the rate of inband management services. Therefore, you can directly bind default traffic profile 6 to the inband management service port.

```
huawei(config)#service-port vlan 8 gpon 0/3/1 ont 1 gemport 11 multi-service
user-vlan 8 rx-cttr 6 tx-cttr 6
```

Step 7 Check whether the management service port between the OLT and the ONU is available.

- Run the **ping *ONU ip*** command on the OLT to check the connectivity between the OLT and the ONU. If the ICMP ECHO-REPLY packets from the ONU are received, the connectivity between the OLT and the ONU is in good condition.
- If you can remotely log in to the ONU from the OLT to perform configurations for the ONU, the management service port between the OLT and the ONU is available.

----End

Follow-up Procedure

When **Config state** is **failed**, **Run state** is **offline**, or **Match state** is **mismatch**:

- If **Control flag** is **deactive**, run the **ont active** command in GPON mode to activate the ONU.
- If **Run state** is **offline**, a physical line may be broken or the optical module may be damaged. Check the line and the optical module.
- If **Config state** is **failed**, the configured ONU capability exceeds the actual ONU capability. In this case, run the **display ont failed-configuration** command in the diagnose mode to check the failed configuration item and the failure cause. Then, rectify the fault accordingly.
- If the ONU does not match, that is, **Match state** is **mismatch**, the port types and number of ports undermatch the actual port types and number of ports supported by the ONU. In this case, run the **display ont capability** command to query the actual capability of the ONU, and then select one of the following modes to modify the ONU configuration:
  - Create a proper ONU profile according to the actual capability of the ONU, and then run the **ont modify** command to modify the configuration data of the ONU.
  - Modify the ONU profile according to the actual capability of the ONU and save the modification. Then, the ONU automatically recovers the configuration successfully.

Copyright © Huawei Technologies Co., Ltd.

14.4.5.4 Configuring the TDM Connection and TDM PW

A TDM connection is created between OLT-A and the ONU and bound to the PW. A TDM connection for the E1 or SHDSL port is created on OLT-B. SPUB boards are used to transmit TDM PWE3 services between the 2 OLTs.

Prerequisites

1. The EDTB board on OLT-B is in position and functions normally.
2. SPUB boards on OLT-A and OLT-B are in position and function normally.

Data Plan

Table 14-9 Key data plan

Item	Data
VLAN	1000
ONU E1 port	● Port ID: 0/1/0 ● Port signaling mode: unstructured data transfer (UDT) ● Transmit clock of the port: system clock
E1 or SHDSL port parameters on OLT-B	Slot for the EDTB board: 0/2 Port ID for E1 access: 0/2/0 Port ID for SHDSL access: 0/2/16 Transmit clock of the port: system clock
IP address	OLT-A: ● IP address of the VLAN interface: 10.0.0.10/24 ● IP address of the loopback interface: 1.1.1.1/32 OLT-B: ● IP address of the VLAN interface: 10.0.0.20/24 ● IP address of the loopback interface: 2.2.2.2/32
PW parameters	The following parameters must be the same on the 2 OLTs. ● PW ID: 1 ● PW type: TDM SAToP E1 ● Control word: enabled ● PW load time: 125 μs ● Size of jitter buffer: 500 μs ● RTP header: enabled

Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Configure the TDM connection.

OLT-A adopts GPON access. TDM connections need to be configured on the ONU and OLT-A separately.

1. Configure the TDM virtual channel link (VCL) on the ONU.

   On GPON port 0/3/1, create the TDM VCL for E1 port 0/1/0 of ONU 0.

   NOTE

   Each E81A board has 8 E1 ports. Port IDs 0 to 7 on board 0/1 correspond to ONT port IDs 1 to 8, port IDs 0 to 7 on board 0/2 correspond to ONT port IDs 9 to 16, and so forth.

   ```
   huawei(config-if-gpon-0/3)ont tdm-vcl 1 0 tdm-vcl-id 0 satop 1
   huawei(config-if-gpon-0/3)quit
   ```

2. Configure the TDM connection on OLT-A.

   ```
   huawei(config)tdm-connect connectid 0 tdm pwe3-uplink gpon 0/3/1 ontid 1
   gemportIndex 13 tdm-vcl 0
   ```

OLT-B adopts E1 or SHDSL access. The following shows how to configure the TDM connection.

- For E1 access:

  ```
  huawei(config)#interface edt 0/2
  huawei(config-if-edt-0/2)#board workmode satop   //The EDTB board must work in
  the SAToP mode.
    Success: Set the board workmode success
  huawei(config-if-edt-0/2)#quit
  huawei(config)#tdm-connect connectid 0 tdm pwe3-uplink 0/2 e1 0/2/0
  ```

- For SHDSL access:

  ```
  huawei(config)#interface edt 0/2
  huawei(config-if-edt-0/2)#board workmode satop
    Success: Set the board workmode success
  huawei(config-if-edt-0/2)#quit
  huawei(config)#tdm-connect connectid 0 tdm pwe3-uplink 0/2 shdsl 0/2/16
  ```

Step 2 Configure the basic functions of multiprotocol label switching (MPLS).

1. Create VLAN 1000, add the upstream port into VLAN 1000, and configure the IP address of VLAN interface 1000.

   ```
   huawei(config)#vlan 1000 smart
   huawei(config)#port vlan 1000 0/19 0
   huawei(config)#interface vlanif 1000
   huawei(config-if-vlanif1000)#ip address 10.0.0.10 24
   ```

2. Configure the IP address of the loopback interface and MPLS LSR ID.

   ```
   huawei(config)#interface loopback 0
   huawei(config-if-loopback0)#ip address 1.1.1.1 32
   huawei(config)#mpls lsr-id 1.1.1.1
   ```

3. Enable MPLS, MPLS L2VPN, and MPLS LDP globally, and then enable MPLS and MPLS LDP for the VLAN interface.

   ```
   huawei(config)#mpls
   Info: Mpls starting, please wait... OK!
   huawei(config-mpls)#quit
   huawei(config)#mpls l2vpn
   huawei(config)#mpls ldp
   huawei(config)#mpls vlan 1000
   huawei(config)#interface vlanif 1000
   huawei(config-if-vlanif1000)#mpls
   huawei(config-if-vlanif1000)#mpls ldp
   ```


Copyright © Huawei Technologies Co., Ltd.

4. Configure a static route to the peer OLT.

   Configure a static route from OLT-A to OLT-B.

   ```
   huawei(config)#ip route-static 2.2.2.2 32 10.0.0.20
   ```

   Configure a static route from OLT-B to OLT-A.

   ```
   huawei(config)#ip route-static 1.1.1.1 32 10.0.0.10
   ```

   After the static routes are configured successfully, ping the VLAN interface or LSR ID of the peer OLT from one OLT. Normally, the ICMP ECHO-REPLY packets from the peer OLT can be received.

Step 3 Configure the MPLS PW.

PW parameter **peer-address** (configured on the 2 OLTs) is set to the LSR ID of the peer OLT, and other PW parameters must be set identically on the 2 OLTs.

```
huawei(config)#pw-para 1
huawei(config-pw-para-1)#peer-address 1.1.1.1  //Set the peer address to the LSR ID
of the peer OLT.
huawei(config-pw-para-1)#pw-type tdm satop e1  //The PW type must be the same as
the attribute of the E1 port on the ONU.
                                               //Configure the SAToP encapsulation,
and set the E1 port signaling mode to UDT.
huawei(config-pw-para-1)#control-word
huawei(config-pw-para-1)#tdm-load-time satop e1 loadtime 125
huawei(config-pw-para-1)#jitter-buffer buffer-size 500
huawei(config-pw-para-1)#rtp-header encap payload-type 0 sn 0 ssrc rcv 0 tx 0
huawei(config-pw-para-1)#quit
```

Step 4 Dynamically bind PW 1 to the TDM connection.

```
huawei(config)#pw-ac-binding tdm 0 pw 1
```

Step 5 Configure the attributes of the E1 port on the ONU.

Log in to the ONU from the OLT, and then configure the port signaling mode of E1 port 0/1/0 to **UDT** and the transmit clock to **system**.

```
huawei(config)#interface tdm 0/1
huawei(config-if-tdm-0/1)#port 0 udt system
huawei(config-if-tdm-0/1)#quit
```

Step 6 (Optional) Configure the attributes of the E1 or SHDSL port on OLT-B.

By default, the transmit clock of the E1 or SHDSL port is the system clock, and therefore the configuration of the transmit clock is not required.

- For E1 access:

  ```
  huawei(config)#interface edt 0/2
  huawei(config-if-edt-0/2)#clock-work 0 system   //The clock of the E1 port is
  the system clock.
  ```

- For SHDSL access:

  ```
  huawei(config)#interface edt 0/2
  huawei(config-if-edt-0/2)#tdm-clock clock-recovery-mode 0 retiming
  ```

----End

Follow-up Procedure

After all the configurations are performed successfully, the related information about the CESoP connection can be queried by running the **display cesop-connect** command on the ONU.

```
huawei(config)#display cesop-connect all
  ------------------------------------------------------------------------------
  ID     PORT VCL ENCAP      REMOTEMAC        REMOTEIP LOCALUDP   REMOTEUDP VLAN
              ID  TYPE                                /RXPWLABEL  /TXPWLABEL
```


Copyright © Huawei Technologies Co., Ltd.

```
------------------------------------------------------------------------------
0   0/1 /0    0  MPLS e024-7f98-a21b              -    9343        8192  TOE
------------------------------------------------------------------------------
Total: 1
```

14.4.5.5 Configuring Clock Synchronization

In this scenario, network-wide clock synchronization is implemented through synchronous Ethernet clocks.

Prerequisites

- The clock daughter board CKMC/CKMD of the SCU control board is in position.
- The Ethernet upstream board is the GICK/GSCA (GE port) or X2CS/SPUF (10GE port) board.
- The upstream MAN PSN of the OLT supports Synchronous Ethernet.

Data Plan

Item	Data
Ethernet upstream board	Port: 0/19/0 **NOTE** The SPUF board exclusively occupies a service slot. This topic uses the GIU upstream board as an example.

Procedure

- **Configure the OLT-side clock.**
  1. Configure a system clock source.

     Use the Ethernet line clock input from GIU port 0/19/0 as the system clock. Set the index of the system clock to **0** and priority to **0** (highest priority).

     ```
     huawei(config)#clock source 0 0/19/0
     huawei(config)#clock priority system 0
     ```

  2. Query the configurations and status of the system clock source.

     Run the **display clock source system** command to query the configurations and status of the clock source. Ensure that the configurations of the system clock source are correct and the status of the system clock source is **Normal**.

     ```
     huawei(config)#display clock source system

     ------------------------------------------------------------------------
     -----
       Index  Board    Source   Clk-type  State       Priority QL
     Selected

     ------------------------------------------------------------------------
     -----
         0    H801GICK 0/19/0    ETH      Normal      0        ---
     YES

     ------------------------------------------------------------------------
     -----
     ```


Copyright © Huawei Technologies Co., Ltd.

Run the **display clock mode** command to query the working mode of the clock. Ensure that the working mode of the clock daughter board is **Tracing**.

```
huawei(config)#display clock mode
  Clock manage-mode:Third-mode
  Clock subboard work-mode:Tracing
```

- **Configure the ONU-side clock.**

  1. Configure the PON line clock as the system clock.

     ```
     huawei(config)#clock source 0 0/0/1
     huawei(config)#clock priority system 0
     ```

  2. Query the configuration and status of the system clock source.

     Run the **display clock source** command to query the configuration and status of the system clock source.

     ```
     huawei(config-if-tdm-0/1)#quit
     huawei(config)#display clock source
       ------------------------------------------------------------------------
       Index  Type   Source      State          Priority     QL    Selected
       ------------------------------------------------------------------------
         0    line   0/0/1       Normal           0          ---       YES
         1    --     -/ -/ -     ---              ---        NO        ---
         2    --     -/ -/ -     ---              ---        NO        ---
         3    --     -/ -/ -     ---              ---        NO        ---
         4    --     -/ -/ -     ---              ---        NO        ---
         5    --     -/ -/ -     ---              ---        NO        ---
         6    --     -/ -/ -     ---              ---        NO        ---
         7    --     -/ -/ -     ---              ---        NO        ---
         8    --     -/ -/ -     ---              ---        NO        ---
         9    --     -/ -/ -     ---              ---        NO        ---
       ------------------------------------------------------------------------
     ```

----End

14.4.5.6 Configuring E2E Reliability

This topic describes how to configure end-to-end (E2E) protection schemes for the enterprise private line service which has a high requirement on service reliability.

Context

Reliability covers equipment reliability, upstream networking protection, and downstream networking protection. For details on reliability data planning, see **13.2.6 Principle of Reliability Data Plan**.

- Upstream networking protection includes link aggregation group and protection group. Usually, link aggregation group is configured when the GIU board is used to transmit traffic upstream; protection group is configured when the main control board is used to transmit traffic upstream. The two protection schemes are not configured at the same time.
- Downstream networking protection includes Type B, Type C single homing, and Type C dual homing, which are used to protect service ports. Ports on the same ONU can be configured only with the same protection scheme.

NOTE

This topic describes how to configure five mainstream protection schemes. Select required protection schemes based on the carrier's requirement and actual networking scenario.

Procedure

- Configure a link aggregation group.

Copyright © Huawei Technologies Co., Ltd.

Bind upstream ports 0/19/0 and 0/19/1 together as an aggregation link group. Each member port in the group transmits packets based on source MAC addresses. The working mode is LACP static aggregation.

```
huawei(config)#link-aggregation 0/19 0-1 ingress workmode lacp-static
```

- Configure a protection group.

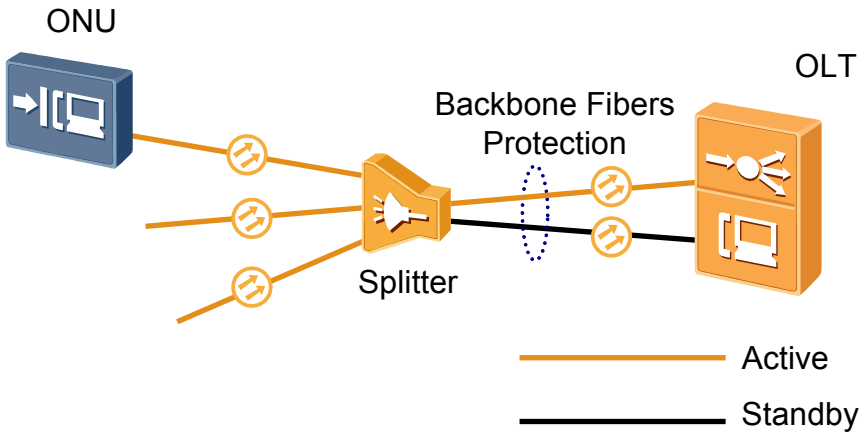
  Configure upstream ports 0/19/0 and 0/19/1 on board GIU as a port protection group. Set port 0/19/0 as the working port and port 0/19/1 as the protection port, set the working mode to time delay detection, and enable the protection group.

```
huawei(config-protect)#protect-group first 0/19/0 second 0/19/1 eth workmode timedelay enable
```

- Configure the Type B protection.

  Figure 14-26 shows the Type B protection networking diagram.

Figure 14-26 Type B protection



Configure redundancy backup for ports 0/3/1 and 0/3/2 on the same GPON board on OLT. When port 0/3/1 fails, the system can automatically switch to port 0/3/2.

```
huawei(config)#protect-group 0 protect-target gpon-uni-port workmode timedelay
huawei(protect-group-0)#protect-group member port 0/3/1 role work
huawei(protect-group-0)#protect-group member port 0/3/2 role protect
huawei(protect-group-0)#protect-group enable
```

NOTE

The configurations of services accessed by the ONUs remain the same after the Type B protection is configured. That is, the service configurations are applied only to the working GPON port.

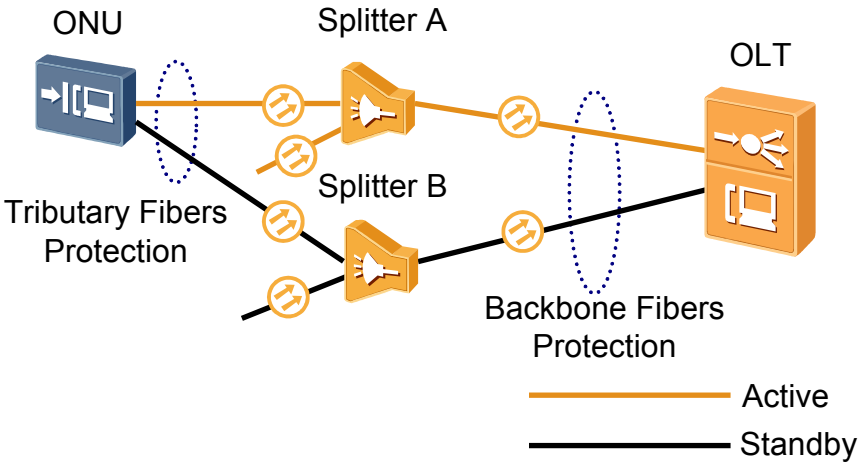
- Configure the Type C single homing protection.

  Figure 14-27 shows networking diagram for the Type C single homing protection. Configure two 1:N optical splitters, one for connecting the working PON ports on the OLT and ONUs, and one for connecting the protection PON ports on the OLT and ONUs. This protection scheme protects both the backbone fibers and tributary fibers.

  The configurations of services accessed by the ONUs remain the same after the Type C single homing protection is configured. That is, the service configurations are applied only to the working PON port on the OLT and working upstream PON ports on the ONUs.

Copyright © Huawei Technologies Co., Ltd.

Figure 14-27 Type C single homing protection



As shown in the preceding figure, Type C single homing protecting is configured for optical fiber links between the OLT and ONU.

- The ports on the GPON service board are 0/3/1 and 0/3/2.
- The link at port 0/3/1 is the working link.
- The link at port 0/3/2 is the protection link.
- The ONU ID is 1.
- The ONU is authenticated by serial number (SN). The SN of the ONU is 32303131B39FD641 and the management mode is SNMP.
- The ID of the line profile bound to the ONU is 10.

```
huawei(config)#interface gpon 0/3
huawei(config-if-gpon-0/3)#ont add 1 1 sn-auth 32303131B39FD641 snmp ont-lineprofile-id 10
huawei(config-if-gpon-0/3)#ont add 2 1 protect-side
huawei(config-if-gpon-0/3)#quit
huawei(config)#protect-group protect-target gpon-uni-ont workmode portstate
huawei(protect-group-1)#protect-group member port 0/3/1 ont 1 role work
huawei(protect-group-1)#protect-group member port 0/3/2 ont 1 role protect
huawei(protect-group-1)#protect-group enable
huawei(protect-group-1)#quit
```

- Configure the Type C dual homing protection.

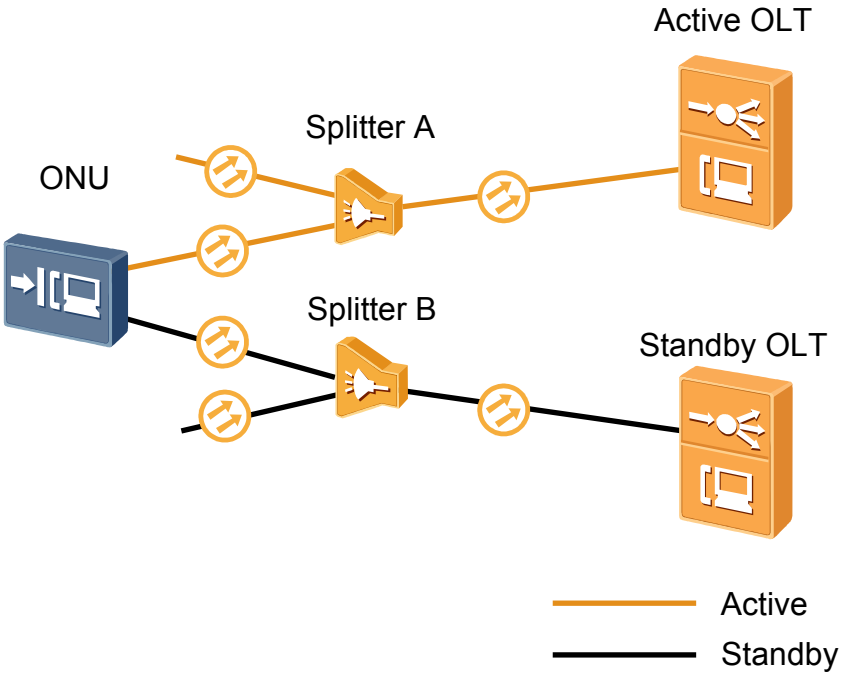
  Figure 14-28 shows the networking diagram for the Type C dual homing protection. Two PON ports on different OLTs, two PON ports on an ONU, two backbone optical fibers, two optical splitters, and two tributary optical fibers are configured to implement this protection. The difference between this protection scheme and the Type C single homing protection scheme is that the ONU needs to be dual homed to two OLTs in this protection scheme.

  The models and versions of main control boards on the active and standby OLTs must be the same. The models and versions of GPON boards on the active and standby OLTs also must be the same. Data on the active OLT cannot be automatically synchronized with that on the standby OLT. Therefore, data synchronization between the active and standby OLTs must be manually ensured.

  This protection scheme can be configured for only the Ethernet QinQ private line service. It does not support TDM services, including Native TDM and SAToP.

Copyright © Huawei Technologies Co., Ltd.

Figure 14-28 Type C dual homing protection



As shown in the preceding figure, Type C dual homing protection is configured for two OLTs (huawei_A and huawei_B).

- huawei_A is the active OLT while huawei_B is the standby OLT.
- The ports on the service boards on both OTLs are 0/3/1.
- The dual homing protection group ID is 1.
- The ONU ID is 1.
- The ONU is authenticated by serial number (SN). The SN of the ONU is 32303131B39FD641 and the management mode is SNMP.
- The ID of the line profile bound to the ONU is 10.

```
Configurations on the active OLT huawei_A:
huawei_A(config)#interface gpon 0/3
huawei_A(config-if-gpon-0/3)#ont add 1 1 sn-auth 32303131B39FD641 snmp ont-
lineprofile-id 10
huawei_A(config-if-gpon-0/3)#quit
huawei_A(config)#protect-group 1 protect-target gpon-uni-ont workmode dual-
parenting
huawei_A(protect-group-1)#protect-group member port 0/3/1 ont 1 role work
Configurations on the standby OLT huawei_B:
huawei_B(config)#interface gpon 0/3
huawei_B(config-if-gpon-0/3)#ont add 1 1 sn-auth 32303131B39FD641 snmp ont-
lineprofile-id 10
huawei_B(config-if-gpon-0/3)#quit
huawei_B(config)#protect-group 1 protect-target gpon-uni-ont workmode dual-
parenting
huawei_B(protect-group-1)#protect-group member port 0/3/1 ont 1 role protect
huawei_B(protect-group-1)#protect-group enable
```

----End

Copyright © Huawei Technologies Co., Ltd.

14.4.5.7 Verifying Services

Verifying private line services requires a dedicated E1 line test instrument.

Prerequisites

The configuration of private line services has been completed.

Context

Because E1 access is applied to both sides of the packet switched network (PSN), an E1 line test instrument can be used to verify services. The E1 line test instrument is connected to the E1 port of the device on one side of the network after the port loopback or hardware loopback is configured on the E1 port of the device on the other side of the network.

Procedure

Step 1 Configure a local loopback on the E1 port.

If the E1 port of the ONU is used to provide access for the private line services, the configurations are as follows:

```
huawei(config)#interface tdm 0/1
huawei(config-if-tdm-0/1)#loopback 0 local
  This operation will interrupt the service, continue? (y/n)[n]:y
```

If the E1 port of the EDTB board is used to provide access for the private line services, the configurations are as follows:

```
huawei(config)#interface edt 0/2
huawei(config-if-edt-0/2)#loopback 0 local
```

Step 2 Use the E1 line test instrument to send packets.

NOTE

Ensure the synchronization between clocks. It is recommended that the E1 line test instrument should use the self-generated clock, the OLT should trace the clock of the E1 line test instrument, and the ONU should trace the clock of the OLT.

The test duration must be equal to or longer than 12 hours. No alarm information is displayed on the test instrument, and the bit error rate (BER) must be lower than 1E-9.

----End

Follow-up Procedure

You can collect the packet statistics to check whether the CESoP and TDM connections are normal.

- Collect the statistics of packets sent and received by the CESoP connection on the ONU.

```
huawei(config)#display cesop-connect statistics 0
  ------------------------------------------------------
  CONNECTID : 0
  ------------------------------------------------------
  Lost Packet Count:                0
  Received Packet Count:            58733
  Transmitted Packet Count:         58732
  Overflow Jitter Buffer Times:     0
  Underflow Jitter Buffer Times:    0
  Received Abnormal Packet Count:   0
```


Copyright © Huawei Technologies Co., Ltd.

```
  Received Sn-error Packet Count:   0
  Received Ssrc-error Packet Count: 0
  ----------------------------------------------------
```

In the command output, the number of received packets must be the same as that of sent packets.

- Collect the statistics of packets sent and received by the TDM connection on the OLT.

```
huawei(config)#display tdm-connect statistics 0
-------------------------------------------------------------
   Statistics on ONU side:
   Discarded Packets                                : 0
   Received Packets                                 : 132252
   Transmitted Packets                              : 132253
   Received Error CESoP Packets                     : 0
   Received SN Error CESoP Packets                  : 0
   Received SSRC Error CESoP Packets                : 0
  -------------------------------------------------------------
```

In the command output, the number of received packets must be the same as that of sent packets.

14.4.6 Symmetrical E1 or SHDSL Access for OLTs on Both Sides

Signals of enterprise or base transceiver station (BTS) private line services are transmitted to the OLTs on both sides of the packet switched network (PSN) through E1 or SHDSL lines. TDM PWE3 is created between the 2 OLTs to enable the PSN network to carry circuit switched (CS) services.

14.4.6.1 Service Requirements and Application Scenario

Service Requirements

Enhancing O&M capability: The MxU configurations can be performed on the OLT, which simplifies the configuration process.

Minimizing network construction costs: Only 1 EDTB board is required for an OLT.

Allowing TDM services to traverse the packet switched network (PSN): TDM services are deployed independently.

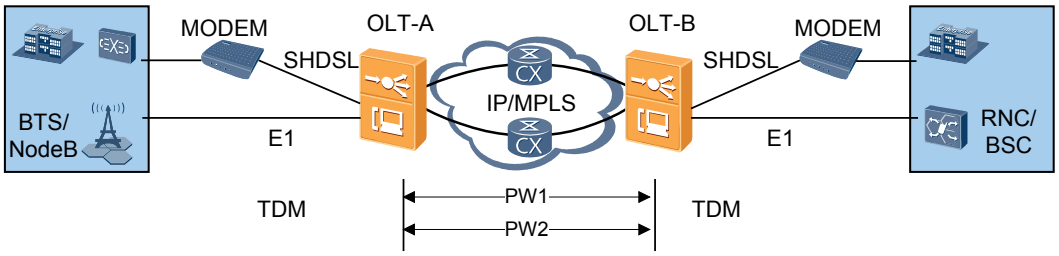
Application Scenario

As shown in **Figure 14-29**, OLT-A and OLT-B are deployed on both sides of the PSN network. Enterprise or base transceiver station (BTS) private line services are transmitted to OLT-A and OLT-B through E1 or SHDSL lines. TDM PWs are created between the 2 OLTs to provide cross-PSN-network access and backhaul for enterprise or BTS private line services.

The model of the ONU supporting this solution is MA5698, MA5898, MA5616.

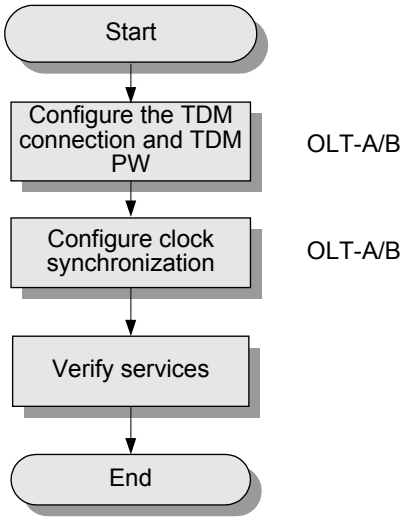
Copyright © Huawei Technologies Co., Ltd.

Figure 14-29 Example network of symmetrical E1 or SHDSL access



14.4.6.2 Configuration Procedure

The following figure shows the procedure of symmetrically configuring E1 or SHDSL access for OLTs on both sides of the packet switched network (PSN). Because OLTs are symmetrically deployed, the configuration steps on the 2 OLTs are the same, but the IP addresses for specific interfaces are different.



14.4.6.3 Configuring the TDM Connection and TDM PW

TDM connections for E1 or SHDSL ports are created on OLT-A and OLT-B. SPUB boards are used to transmit TDM PWE3 services between the 2 OLTs.

Prerequisites

The EDTB and SPUB boards on OLT-A or OLT-B are in position and function normally.

Data Plan

When OLTs are symmetrically connected to the packet switched network (PSN), the configuration steps for OLT-A and OLT-B are the same, and only the configuration data varies

Copyright © Huawei Technologies Co., Ltd.

with the OLTs. The varied configuration data of OLT-A and OLT-B will be separately described in this topic.

Table 14-10 Key data plan

Item	Data
VLAN	1000
E1 or SHDSL port parameters on the OLT	Slot for the EDTB board: 0/2 Port ID for E1 access: 0/2/0 Port ID for SHDSL access: 0/2/16 Transmit clock of the port: system clock
IP address	OLT-A: ● IP address of the VLAN interface: 10.0.0.10/24 ● IP address of the loopback interface: 1.1.1.1/32 OLT-B: ● IP address of the VLAN interface: 10.0.0.20/24 ● IP address of the loopback interface: 2.2.2.2/32
PW parameters	● PW ID: 1 ● PW type: TDM SAToP E1 ● Control word: enabled ● PW load time: 125 μs ● Size of jitter buffer: 500 μs ● RTP header: enabled

Procedure

Step 1 Configure the TDM connection.

Both OLT-A and OLT-B adopt E1 or SHDSL access. The following shows how to configure the TDM connection.

- For E1 access:

```
huawei(config)#interface edt 0/2
huawei(config-if-edt-0/2)#board workmode satop   //The EDTB board must work in
the SAToP mode.
  Success: Set the board workmode success
huawei(config-if-edt-0/2)#quit
huawei(config)#tdm-connect connectid 0 tdm pwe3-uplink 0/2 e1 0/2/0
```

- For SHDSL access:

```
huawei(config)#interface edt 0/2
huawei(config-if-edt-0/2)#board workmode satop
  Success: Set the board workmode success
huawei(config-if-edt-0/2)#quit
huawei(config)#tdm-connect connectid 0 tdm pwe3-uplink 0/2 shdsl 0/2/16
```

Step 2 Configure the basic functions of multiprotocol label switching (MPLS).

Copyright © Huawei Technologies Co., Ltd.

1. Create VLAN 1000, add the upstream port into VLAN 1000, and configure the IP address of VLAN interface 1000.

```
huawei(config)#vlan 1000 smart
huawei(config)#port vlan 1000 0/19 0
huawei(config)#interface vlanif 1000
huawei(config-if-vlanif1000)#ip address 10.0.0.10 24
```

2. Configure the IP address of the loopback interface and MPLS LSR ID.

```
huawei(config)#interface loopback 0
huawei(config-if-loopback0)#ip address 1.1.1.1 32
huawei(config)#mpls lsr-id 1.1.1.1
```

3. Enable MPLS, MPLS L2VPN, and MPLS LDP globally, and then enable MPLS and MPLS LDP for the VLAN interface.

```
huawei(config)#mpls
Info: Mpls starting, please wait... OK!
huawei(config-mpls)#quit
huawei(config)#mpls l2vpn
huawei(config)#mpls ldp
huawei(config)#mpls vlan 1000
huawei(config)#interface vlanif 1000
huawei(config-if-vlanif1000)#mpls
huawei(config-if-vlanif1000)#mpls ldp
```

4. Configure a static route to the peer OLT.

   Configure a static route from OLT-A to OLT-B.

```
huawei(config)#ip route-static 2.2.2.2 32 10.0.0.20
```

   Configure a static route from OLT-B to OLT-A.

```
huawei(config)#ip route-static 1.1.1.1 32 10.0.0.10
```

   After the static routes are configured successfully, ping the VLAN interface or LSR ID of the peer OLT from one OLT. Normally, the ICMP ECHO-REPLY packets from the peer OLT can be received.

Step 3 Configure the MPLS PW.

PW parameter **peer-address** (configured on the 2 OLTs) is set to the LSR ID of the peer OLT, and other PW parameters must be set identically on the 2 OLTs.

```
huawei(config)#pw-para 1
huawei(config-pw-para-1)#peer-address 1.1.1.1  //Set the peer address to the LSR ID
of the peer OLT.
huawei(config-pw-para-1)#pw-type tdm satop e1  //The PW type must be the same as
the attribute of the E1 port on the ONU.
                                               //Configure the SAToP encapsulation,
and set the E1 port signaling mode to UDT.
huawei(config-pw-para-1)#control-word
huawei(config-pw-para-1)#tdm-load-time satop e1 loadtime 125
huawei(config-pw-para-1)#jitter-buffer buffer-size 500
huawei(config-pw-para-1)#rtp-header encap payload-type 0 sn 0 ssrc rcv 0 tx 0
huawei(config-pw-para-1)#quit
```

Step 4 Dynamically bind PW 1 to the TDM connection.

```
huawei(config)#pw-ac-binding tdm 0 pw 1
```

Step 5 (Optional) Configure the attributes of the E1 or SHDSL port.

By default, the transmit clock of the E1 or SHDSL port is the system clock, and therefore the configuration of the transmit clock is not required.

- For E1 access:

Copyright © Huawei Technologies Co., Ltd.

```
huawei(config)#interface edt 0/2
huawei(config-if-edt-0/2)#clock-work 0 system   //The clock of the E1 port is
the system clock.
```

- For SHDSL access:

```
huawei(config)#interface edt 0/2
huawei(config-if-edt-0/2)#tdm-clock clock-recovery-mode 0 retiming
```

----End

Follow-up Procedure

After all the configurations are performed successfully, the related information about the CESoP connection can be queried by running the **display cesop-connect** command on the ONU.

```
huawei(config)#display cesop-connect all
  ------------------------------------------------------------------------------
  ID     PORT VCL ENCAP      REMOTEMAC        REMOTEIP LOCALUDP   REMOTEUDP VLAN
               ID  TYPE                              /RXPWLABEL  /TXPWLABEL
  ------------------------------------------------------------------------------
  0   0/1 /0    0  MPLS e024-7f98-a21b              -    9343        8192  TOE
  ------------------------------------------------------------------------------
  Total: 1
```

14.4.6.4 Configuring Clock Synchronization

In this scenario, network-wide clock synchronization is implemented through synchronous Ethernet clocks.

Prerequisites

- The clock daughter board CKMC/CKMD of the SCU control board is in position.
- The Ethernet upstream board is the GICK/GSCA (GE port) or X2CS/SPUF (10GE port) board.
- The upstream MAN PSN of the OLT supports Synchronous Ethernet.

Data Plan

Item	Data
Ethernet upstream board	Port: 0/19/0 **NOTE** The SPUF board exclusively occupies a service slot. This topic uses the GIU upstream board as an example.

Procedure

- **Configure the OLT-side clock.**
  1. Configure a system clock source.

     Use the Ethernet line clock input from GIU port 0/19/0 as the system clock. Set the index of the system clock to **0** and priority to **0** (highest priority).

     ```
     huawei(config)#clock source 0 0/19/0
     huawei(config)#clock priority system 0
     ```

  2. Query the configurations and status of the system clock source.

Copyright © Huawei Technologies Co., Ltd.

Run the **display clock source system** command to query the configurations and status of the clock source. Ensure that the configurations of the system clock source are correct and the status of the system clock source is **Normal**.

```
huawei(config)#display clock source system

-------------------------------------------------------------------------
-----
  Index  Board    Source   Clk-type  State       Priority QL
Selected

-------------------------------------------------------------------------
-----
    0    H801GICK 0/19/0    ETH      Normal      0        ---
YES

-------------------------------------------------------------------------
-----
```

Run the **display clock mode** command to query the working mode of the clock. Ensure that the working mode of the clock daughter board is **Tracing**.

```
huawei(config)#display clock mode
  Clock manage-mode:Third-mode
  Clock subboard work-mode:Tracing
```

- **Configure the ONU-side clock.**
  1. Configure the PON line clock as the system clock.

     ```
     huawei(config)#clock source 0 0/0/1
     huawei(config)#clock priority system 0
     ```

  2. Query the configuration and status of the system clock source.

     Run the **display clock source** command to query the configuration and status of the system clock source.

     ```
     huawei(config-if-tdm-0/1)#quit
     huawei(config)#display clock source
       ------------------------------------------------------------------------
       Index  Type   Source      State          Priority     QL    Selected
       ------------------------------------------------------------------------
         0    line   0/0/1       Normal           0          ---      YES
         1    --     -/ -/ -     ---              ---        NO       ---
         2    --     -/ -/ -     ---              ---        NO       ---
         3    --     -/ -/ -     ---              ---        NO       ---
         4    --     -/ -/ -     ---              ---        NO       ---
         5    --     -/ -/ -     ---              ---        NO       ---
         6    --     -/ -/ -     ---              ---        NO       ---
         7    --     -/ -/ -     ---              ---        NO       ---
         8    --     -/ -/ -     ---              ---        NO       ---
         9    --     -/ -/ -     ---              ---        NO       ---
       ------------------------------------------------------------------------
     ```

----End

14.4.6.5 Verifying Services

Verifying private line services requires a dedicated E1 line test instrument.

Prerequisites

The configuration of private line services has been completed.

Context

Because E1 access is applied to both sides of the packet switched network (PSN), an E1 line test instrument can be used to verify services. The E1 line test instrument is connected to the E1 port

Copyright © Huawei Technologies Co., Ltd.

of the device on one side of the network after the port loopback or hardware loopback is configured on the E1 port of the device on the other side of the network.

Procedure

Step 1 Configure a local loopback on the E1 port.

If the E1 port of the ONU is used to provide access for the private line services, the configurations are as follows:

```
huawei(config)#interface tdm 0/1
huawei(config-if-tdm-0/1)#loopback 0 local
  This operation will interrupt the service, continue? (y/n)[n]:y
```

If the E1 port of the EDTB board is used to provide access for the private line services, the configurations are as follows:

```
huawei(config)#interface edt 0/2
huawei(config-if-edt-0/2)#loopback 0 local
```

Step 2 Use the E1 line test instrument to send packets.

NOTE

Ensure the synchronization between clocks. It is recommended that the E1 line test instrument should use the self-generated clock, the OLT should trace the clock of the E1 line test instrument, and the ONU should trace the clock of the OLT.

The test duration must be equal to or longer than 12 hours. No alarm information is displayed on the test instrument, and the bit error rate (BER) must be lower than 1E-9.

----End

Follow-up Procedure

You can collect the packet statistics to check whether the CESoP and TDM connections are normal.

- Collect the statistics of packets sent and received by the CESoP connection on the ONU.

```
huawei(config)#display cesop-connect statistics 0
  ----------------------------------------------------
  CONNECTID : 0
  ----------------------------------------------------
  Lost Packet Count:                0
  Received Packet Count:            58733
  Transmitted Packet Count:         58732
  Overflow Jitter Buffer Times:     0
  Underflow Jitter Buffer Times:    0
  Received Abnormal Packet Count:   0
  Received Sn-error Packet Count:   0
  Received Ssrc-error Packet Count: 0
  ----------------------------------------------------
```

  In the command output, the number of received packets must be the same as that of sent packets.

- Collect the statistics of packets sent and received by the TDM connection on the OLT.

```
huawei(config)#display tdm-connect statistics 0
-----------------------------------------------------------------
   Statistics on ONU side:
   Discarded Packets                                : 0
   Received Packets                                 : 132252
   Transmitted Packets                              : 132253
   Received Error CESoP Packets                     : 0
```


Copyright © Huawei Technologies Co., Ltd.

```
  Received SN Error CESoP Packets                    : 0
  Received SSRC Error CESoP Packets                  : 0
-------------------------------------------------------------
```

In the command output, the number of received packets must be the same as that of sent packets.

14.4.7 E1 Access for the ONU and TDM PWE3 Between the ONU and Peer PE

An ONU is connected to the OLT through GPON lines. Signals of enterprise or base transceiver station (BTS) private line services are transmitted to the OLT through the E1 port on the ONU. TDM PWE3 is created between the ONU and the peer provider edge (PE) CX600 to enable the packet switched network (PSN) to carry traditional circuit switched (CS) services.

14.4.7.1 Service Requirements and Application Scenario

Service Requirements

Minimizing network construction costs: No CSPA or SPUB board is required on the OLT.

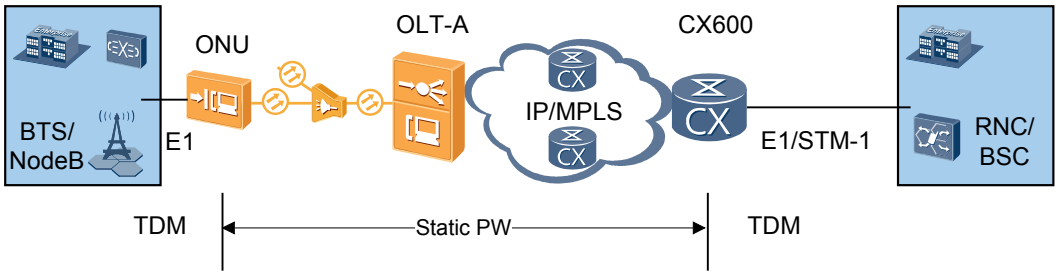
Allowing TDM services to traverse the packet switched network (PSN): TDM services are deployed independently.

Application Scenario

As shown in **Figure 14-30**, an ONU is connected to the OLT through GPON lines. Enterprise or base transceiver station (BTS) private line services are transmitted to the ONU through an E1 port. Static TDM PWs are created between the ONU and the peer provider edge (PE) to provide cross-PSN-network access and backhaul for enterprise or BTS private line services.

The model of the ONU supporting this solution is MA5698, MA5898, MA5616.

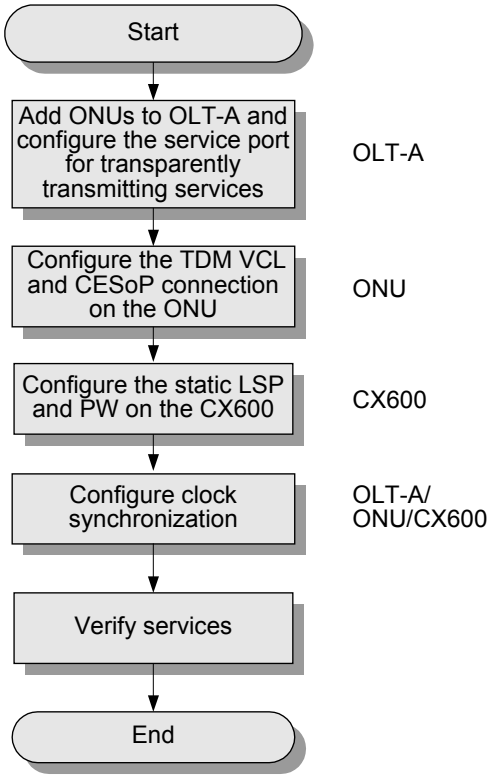
Figure 14-30 Example network of E1 access for the ONU and TDM PWE3 between the ONU and peer PE



14.4.7.2 Configuration Procedure

The following figure shows the procedure of configuring E1 access for the ONU and creating TDM PWE3 between the ONU and peer PE.

Copyright © Huawei Technologies Co., Ltd.



14.4.7.3 Adding ONUs to the OLT and Configuring the Management Service Port

Services can be configured for an ONU only after the ONU is successfully added to the OLT.

Context

- When an ONU is added, related profiles need to be bound to the ONU, including the dynamic bandwidth allocation (DBA) profile, line profile, and alarm profile.
- An ONU can be added in two modes: adding an ONU offline and confirming an ONU online. Select either mode as required.

Data Plan

Table 14-11 Key data plan

Item	Data
DBA profile	Profile ID: 21 Profile type: fixed bandwidth and minimum delay mode DBA bandwidth: 28928 kbit/s (assume that 4 E1 private lines are connected to 1 ONU and each E1 private line is configured with a bandwidth of 7232 kbit/s)

Copyright © Huawei Technologies Co., Ltd.

Item	Data
Line profile	Profile ID: 11 T-CONT ID: 1 GEM port ID for management services: 11 GEM port ID for private line services: 13
Networking data	PON port: 0/3/1 ONU parameters: ● ONU ID: 1 ● SN: 32303131B39FD641
Management VLAN and management IP address	On the OLT: Management VLAN ID: 8 Management VLAN type: smart VLAN Inband management IP address: 192.168.50.1/24 On the ONU: Management VLAN ID: 8 Management VLAN type: smart VLAN Inband management IP address: 192.168.50.2/24
Service VLAN	300
Traffic profile (for transparent transmission)	Index: 10 CIR: off Policy: user-cos; default priority: 7 Priority policy: tag-in-package

Procedure

Step 1 Configure GPON ONU profiles.

1. Configure the DBA profile, and set the DBA bandwidth allocation mode of the GPON port to **min-loop-delay**.

```
huawei(config)#dba-profile add profile-id 21 type1 fix 28928
huawei(config)#interface gpon 0/3
huawei(config-if-gpon-0/3)#port dba bandwidth-assignment-mode 1 min-loop-delay
huawei(config-if-gpon-0/3)#quit
```

2. Configure the ONU line profile.

```
huawei(config)#ont-lineprofile gpon profile-id 11
huawei(config-gpon-lineprofile-11)#tcont 1 dba-profile-id 21  //Bind DBA
profile 21 to T-CONT 1.
huawei(config-gpon-lineprofile-11)#gem add 11 eth tcont 0
huawei(config-gpon-lineprofile-11)#gem add 13 eth tcont 1 //Add GEM port 13 to
T-CONT 1.
huawei(config-gpon-lineprofile-11)#gem mapping 11 0 vlan 8
huawei(config-gpon-lineprofile-11)#gem mapping 13 1 vlan 300 //Map GEM port 13
to VLAN 300.
```


Copyright © Huawei Technologies Co., Ltd.

```
huawei(config-gpon-lineprofile-11)#commit
huawei(config-gpon-lineprofile-11)#quit
```

3. (Optional) Configure the alarm profile.
   - The ID of the default GPON alarm profile is 1. The thresholds for all the alarm parameters in the default alarm profile are 0, which indicates that no alarm is generated.
   - In this example, the default alarm profile is used, and therefore the configuration of the alarm profile is not required.

Step 2 Add an ONU to the OLT.

1. Add ONU 1 offline.

```
huawei(config)#interface gpon 0/3
huawei(config-if-gpon-0/3)#ont add 1 ontid 1 sn-auth 32303131B39FD641
snmp ont-lineprofile-id 11
```

2. (Optional) Bind the alarm profile to ONU 1.

   By default, alarm profile 1 is automatically bound to the ONU. You need to manually bind a non-default alarm profile to the ONU only when the default one does not meet the requirement.

   In this example, default alarm profile 1 is used, and therefore the configuration of the alarm profile is not required.

Step 3 Check the ONU status.

After the ONU is added, run the **display ont info** command to query the status of the ONU. Ensure that **Config flag** of the ONU is **active**, **Run State** is **online**, and **Config state** is **normal**.

To query the status of ONU 1, do as follows:

```
huawei(config-if-gpon-0/3)#display ont info 1 1
  ------------------------------------------------------------------------
  F/S/P                : 0/3/1
  ONT-ID               : 1
  Control flag         : active    //Indicates that the ONU is
activated.
  Run state            : online    //Indicates that the ONU goes online
normally.
  Config state        : normal    //Indicates that the configuration recovery state
of the ONU is normal.
...//The following command output is omitted.
huawei(config-if-gpon-0/3)#quit
```

Step 4 Configure the inband management VLAN and IP address of the OLT.

Create a VLAN whose ID is 8 as the inband management VLAN of the OLT, set the VLAN priority to 6, and set the IP address of the VLAN interface to 192.168.50.1/24.

```
huawei(config)#vlan 8 smart
huawei(config)#vlan priority 8 6
huawei(config)#port vlan 8 0/19 0
huawei(config)#interface vlanif 8
huawei(config-if-vlanif8)#ip address 192.168.50.1 24
huawei(config-if-vlanif8)#quit
```

Step 5 Configure the inband management VLAN and IP address of the ONU.

```
huawei(config)#interface gpon 0/3
huawei(config-if-gpon-0/3)#ont ipconfig 1 1 static ip-address 192.168.50.2 mask
255.255.255.0 gateway
192.168.50.1 vlan 8
huawei(config-if-gpon-0/3)#quit
```


Copyright © Huawei Technologies Co., Ltd.

Step 6 Configure an inband management service port.

The management VLAN is VLAN 8, the GEM port ID is 11, and user VLAN is VLAN 8. The OLT does not limit the rate of inband management services. Therefore, you can directly bind default traffic profile 6 to the inband management service port.

```
huawei(config)#service-port vlan 8 gpon 0/3/1 ont 1 gemport 11 multi-service
user-vlan 8 rx-cttr 6 tx-cttr 6
```

Step 7 Check whether the management service port between the OLT and the ONU is available.

- Run the **ping *ONU ip*** command on the OLT to check the connectivity between the OLT and the ONU. If the ICMP ECHO-REPLY packets from the ONU are received, the connectivity between the OLT and the ONU is in good condition.
- If you can remotely log in to the ONU from the OLT to perform configurations for the ONU, the management service port between the OLT and the ONU is available.

Step 8 Configure the traffic profile and create the service port for transparently transmitting services.

Set the service VLAN (SVLAN) ID to 300, GEM port ID to 13, and customer VLAN (CVLAN) ID to 300. The OLT does not limit the rate of services that are transparently transmitted. Traffic profile 10 is bound to the service port for transparently transmitting services.

```
huawei(config)#traffic table ip index 10 cir off priority user-cos 7 priority-
policy tag-In-package
huawei(config)#service-port vlan 300 gpon 0/3/1 ont 1 gemport 13 multi-service
user-vlan 300 rx-cttr 10 tx-cttr 10
```

----End

Follow-up Procedure

When **Config state** is **failed**, **Run state** is **offline**, or **Match state** is **mismatch**:

- If **Control flag** is **deactive**, run the **ont active** command in GPON mode to activate the ONU.
- If **Run state** is **offline**, a physical line may be broken or the optical module may be damaged. Check the line and the optical module.
- If **Config state** is **failed**, the configured ONU capability exceeds the actual ONU capability. In this case, run the **display ont failed-configuration** command in the diagnose mode to check the failed configuration item and the failure cause. Then, rectify the fault accordingly.
- If the ONU does not match, that is, **Match state** is **mismatch**, the port types and number of ports undermatch the actual port types and number of ports supported by the ONU. In this case, run the **display ont capability** command to query the actual capability of the ONU, and then select one of the following modes to modify the ONU configuration:
  - Create a proper ONU profile according to the actual capability of the ONU, and then run the **ont modify** command to modify the configuration data of the ONU.
  - Modify the ONU profile according to the actual capability of the ONU and save the modification. Then, the ONU automatically recovers the configuration successfully.

14.4.7.4 Configuring the TDM VCL and CESoP Connection on the ONU

Copyright © Huawei Technologies Co., Ltd.

Data Plan

Item	Data
E1 port parameters	Port ID: 0/1/0 Port signaling mode: structured data transfer (SDT) Transmit clock of the port: system clock Port signaling: common channel signaling (CCS) CRC-4 frame check: enabled IP address: 10.0.0.10 Port timeslot: 1-15 (timeslot bitmap: 0xfffe)
Service VLAN	300
Static LSP parameters	Tx LSP label: 2000 Rx LSP label: 8200
Static PW parameters **NOTE** The PW parameters on the ONU must be the same as those on the CX600.	Tx PW label: 8000 Rx PW label: 8500 RTP header: enabled PW load time: 1000 μs Maximum jitter delay: 2 ms

Procedure

Step 1 Create the service VLAN and add an upstream port to the VLAN.

```
huawei(config)#vlan 300 smart
huawei(config)#port vlan 300 0/0 0
```

Step 2 Configure the attributes of the E1 Port.

```
huawei(config)#interface tdm 0/1
huawei(config-if-tdm-0/1)#port 0 sdt system ccs crc enable
huawei(config-if-tdm-0/1)#set ip-address 10.0.0.10
huawei(config-if-tdm-0/1)#quit
```

Step 3 Configure the TDM virtual channel link (VCL).

Set the TDM VCL ID to 0 and the type to CESoP, and use timeslot 1-16.

```
huawei(config)#tdm-vcl tdm-vcl-id 0 cesop 0/1/0 timeslot 0xfffe
```

Step 4 Configure the CESoP connection.

Use VLAN 300 to carry CESoP services. Set the Rx PW label to 8500, Tx PW label to 8000, Rx LSP label to 8200, Tx LSP label to 2000, and gateway IP address (the next hop is the CX600) to 10.0.0.20. Then configure the specific attributes of the CESoP connection.

```
huawei(config)#cesop-connect 1 tdm 0 vlan 300 rcv-pw-label 8500 trans-pw-label
8000
rcv-lsp-label 8200 trans-lsp-label 2000 gateway 10.0.0.20
huawei(config)#cesop rtp 1 enable   //Enable RTP header.
huawei(config)#cesop loadtime 1 1000    //The load time is 1000 μs (namely 8
frames).
```


Copyright © Huawei Technologies Co., Ltd.

```
huawei(config)#cesop jitter-buffer 1 2000   //The maximum jitter delay is 2 ms.
huawei(config)#cesop encap 0 ssrc rcv 0 tx 0   //Both the Tx and Rx SSRIDs are 0.
```

----End

14.4.7.5 Configuring the Static LSP and PW on the CX600

Data Plan

Item	Data
Parameters of the GE sub interface	Sub interface ID: 1/0/0.1 VLAN to which the sub interface belongs: 300 IP address of the sub interface: 10.0.0.20/24
E1 port parameters	Port ID: 2/1/0 Working mode: channelized mode (CEL) Timeslot: 1-15
Static LSP parameters	Parameters configured on the ingress node: ● Destination ID address: 10.0.0.10/32 ● Next-hop IP address: 10.0.0.10 ● Egress interface: GE sub interface 1/0/0.1 ● Egress label: 8200 (the same as the Rx LSP label on the ONU) Parameters configured on the egress node: ● Ingress interface: GE sub interface 1/0/0.1 ● Ingress label: 2000 (the same as the Tx LSP label on the ONU)
Static PW parameters **NOTE** The PW parameters on the CX600 must be the same as those on the ONU.	Tx PW label: 8500 (the same as the Rx PW label on the ONU) Rx PW label: 8000 (the same as the Tx PW label on the ONU) RTP header: enabled Number of TDM frames encapsulated in each PW packet: 8 Maximum jitter delay: 2 ms

Procedure

Step 1 Configure the GE sub interface.

Set the ID of the sub interface to 1/0/0.1, add the sub interface to VLAN 300, and set the IP address of the sub interface to 10.0.0.20/24.

```
[CX600]interface GigabitEthernet 1/0/0.1
[CX600-GigabitEthernet1/0/0.1]vlan-type dot1q 300
[CX600-GigabitEthernet1/0/0.1]ip address 10.0.0.20 24
[CX600-GigabitEthernet1/0/0.1]quit
```

Enable MPLS globally and then enable MPLS for the GE sub interface.

Copyright © Huawei Technologies Co., Ltd.

```
[CX600]mpls
[CX600]interface GigabitEthernet 1/0/0.1
[CX600-GigabitEthernet1/0/0.1]mpls
```

Step 2 Configure the E1 port.

Configure E1 port 2/1/0. Set the working mode to **CEL** and timeslot 1-15 as a channel.

NOTE

The timeslot on the CX600 must be the same as that on the ONU.

```
[CX600]controller E1 2/1/0
[CX600-E1 2/1/0]using ce1
[CX600-E1 2/1/0]channel-set 0 timeslot-list 1-15
[CX600-E1 2/1/0]quit
```

Step 3 Configure the static route to the ONU.

Configure the static route whose destination IP address is the IP address of the E1 board on the ONU and egress interface is GE sub interface 1/0/0.1.

```
[CX600]ip route-static 10.0.0.10 32 GigabitEthernet 1/0/0.1 10.0.0.10
```

Step 4 Configure the CX600 as the ingress node of the static LSP.

```
[CX600]static-lsp ingress lsp1 destination 10.0.0.10 32 nexthop 10.0.0.10
 outgoing-interface GigabitEthernet 1/0/0.1 out-label 8200
```

Step 5 Configure the CX600 as the egress node of the static LSP.

```
[CX600]static-lsp egress lsp2 incoming-interface GigabitEthernet 1/0/0.1
 in-label 2000
```

Step 6 Configure the static PW.

```
[CX600]interface Serial2/1/0:0
[CX600-Serial2/1/0:0]link-protocol tdm
[CX600-Serial2/1/0:0]mpls static-l2vc destination 10.0.0.10 transmit-vpn
-label 8500 receive-vpn-label 8000 rtp-header tdm-encapsulation 8 jitter-buffer 2
```

----End

14.4.7.6 Configuring Clock Synchronization

In this scenario, network-wide clock synchronization is implemented through synchronous Ethernet clocks.

Prerequisites

- The clock daughter board CKMC/CKMD of the SCU control board is in position.
- The Ethernet upstream board is the GICK/GSCA (GE port) or X2CS/SPUF (10GE port) board.
- The upstream MAN PSN of the OLT supports Synchronous Ethernet.

Copyright © Huawei Technologies Co., Ltd.

Data Plan

Item	Data
Ethernet upstream board	Port: 0/19/0 **NOTE** The SPUF board exclusively occupies a service slot. This topic uses the GIU upstream board as an example.

Procedure

- **Configure the OLT-side clock.**
  1. Configure a system clock source.

     Use the Ethernet line clock input from GIU port 0/19/0 as the system clock. Set the index of the system clock to **0** and priority to **0** (highest priority).

     ```
     huawei(config)#clock source 0 0/19/0
     huawei(config)#clock priority system 0
     ```

  2. Query the configurations and status of the system clock source.

     Run the **display clock source system** command to query the configurations and status of the clock source. Ensure that the configurations of the system clock source are correct and the status of the system clock source is **Normal**.

     ```
     huawei(config)#display clock source system

     ------------------------------------------------------------------------
     -----
       Index  Board    Source   Clk-type  State       Priority QL
     Selected

     ------------------------------------------------------------------------
     -----
         0    H801GICK 0/19/0    ETH      Normal      0        ---
     YES

     ------------------------------------------------------------------------
     -----
     ```

     Run the **display clock mode** command to query the working mode of the clock. Ensure that the working mode of the clock daughter board is **Tracing**.

     ```
     huawei(config)#display clock mode
       Clock manage-mode:Third-mode
       Clock subboard work-mode:Tracing
     ```

- **Configure the ONU-side clock.**
  1. Configure the PON line clock as the system clock.

     ```
     huawei(config)#clock source 0 0/0/1
     huawei(config)#clock priority system 0
     ```

  2. Query the configuration and status of the system clock source.

     Run the **display clock source** command to query the configuration and status of the system clock source.

     ```
     huawei(config-if-tdm-0/1)#quit
     huawei(config)#display clock source
       ------------------------------------------------------------------
       Index  Type   Source      State         Priority     QL    Selected
       ------------------------------------------------------------------
         0    line   0/0/1       Normal          0          ---      YES
     ```


Copyright © Huawei Technologies Co., Ltd.

```
  1    --     -/ -/ -     ---            ---        NO       ---
  2    --     -/ -/ -     ---            ---        NO       ---
  3    --     -/ -/ -     ---            ---        NO       ---
  4    --     -/ -/ -     ---            ---        NO       ---
  5    --     -/ -/ -     ---            ---        NO       ---
  6    --     -/ -/ -     ---            ---        NO       ---
  7    --     -/ -/ -     ---            ---        NO       ---
  8    --     -/ -/ -     ---            ---        NO       ---
  9    --     -/ -/ -     ---            ---        NO       ---
-------------------------------------------------------------------------
```

----End

14.4.7.7 Verifying Services

Verifying private line services requires a dedicated E1 line test instrument.

Prerequisites

The configuration of private line services has been completed.

Context

Because E1 access is applied to both sides of the packet switched network (PSN), an E1 line test instrument can be used to verify services. The E1 line test instrument is connected to the E1 port of the device on one side of the network after the port loopback or hardware loopback is configured on the E1 port of the device on the other side of the network.

Procedure

Step 1 Configure a local loopback on the E1 port.

If the E1 port of the ONU is used to provide access for the private line services, the configurations are as follows:

```
huawei(config)#interface tdm 0/1
huawei(config-if-tdm-0/1)#loopback 0 local
  This operation will interrupt the service, continue? (y/n)[n]:y
```

If the E1 port of the EDTB board is used to provide access for the private line services, the configurations are as follows:

```
huawei(config)#interface edt 0/2
huawei(config-if-edt-0/2)#loopback 0 local
```

Step 2 Use the E1 line test instrument to send packets.

NOTE

Ensure the synchronization between clocks. It is recommended that the E1 line test instrument should use the self-generated clock, the OLT should trace the clock of the E1 line test instrument, and the ONU should trace the clock of the OLT.

The test duration must be equal to or longer than 12 hours. No alarm information is displayed on the test instrument, and the bit error rate (BER) must be lower than 1E-9.

----End

Copyright © Huawei Technologies Co., Ltd.

Follow-up Procedure

You can collect the packet statistics to check whether the CESoP and TDM connections are normal.

- Collect the statistics of packets sent and received by the CESoP connection on the ONU.

```
huawei(config)#display cesop-connect statistics 0
  ------------------------------------------------------
  CONNECTID : 0
  ------------------------------------------------------
  Lost Packet Count:                0
  Received Packet Count:            58733
  Transmitted Packet Count:         58732
  Overflow Jitter Buffer Times:     0
  Underflow Jitter Buffer Times:    0
  Received Abnormal Packet Count:   0
  Received Sn-error Packet Count:   0
  Received Ssrc-error Packet Count: 0
  ------------------------------------------------------
```

  In the command output, the number of received packets must be the same as that of sent packets.

- Collect the statistics of packets sent and received by the TDM connection on the OLT.

```
huawei(config)#display tdm-connect statistics 0
-----------------------------------------------------------------
   Statistics on ONU side:
   Discarded Packets                                : 0
   Received Packets                                 : 132252
   Transmitted Packets                              : 132253
   Received Error CESoP Packets                     : 0
   Received SN Error CESoP Packets                  : 0
   Received SSRC Error CESoP Packets                : 0
  -----------------------------------------------------------------
```

  In the command output, the number of received packets must be the same as that of sent packets.

14.4.8 Small-Cell Base Station Access Service (in QinQ VLAN through CLI Configuration)

Dock ONUs are connected to small-cell base stations through Ethernet ports, and OLTs interconnect with the devices on the metro network through QinQ VLANs to provide the access service for small-cell base stations. This topic describes how to implement the access service of a small-cell base station through the CLI in the scenario without the U2000 NMS.

14.4.8.1 Service Requirements and Application Scenarios

Service Requirements

As the last mile that connects users to the Internet, small-cell backhaul is an important part of an FTTx network. For small-cell backhaul, customers expect to:

- Make full use of the existing access resources to provide backhaul services for distributed small-cell base stations.
- Use a simple and mature service configuration scheme, featuring a high transmission efficiency in addition to ensuring the QoS.
- Simplify sites to lower the site installation and maintenance costs.

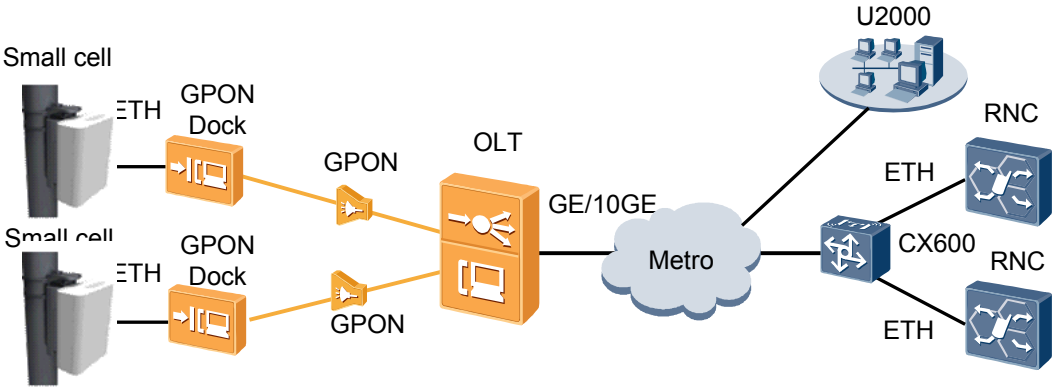
Copyright © Huawei Technologies Co., Ltd.

Application Scenarios

As shown in **Figure 14-31**, ONUs, functioning as Dock devices, receive Ethernet service data from small-cell base stations through Ethernet ports and then send the service data to the OLT. The OLT restores the Ethernet signals and adds 2 VLAN tags (QinQ VLAN encapsulation) to the data, so that the data from the small-cell base stations can be transparently transmitted to the peer PTN devices through the public network and then the PTN devices restore them to the original data.

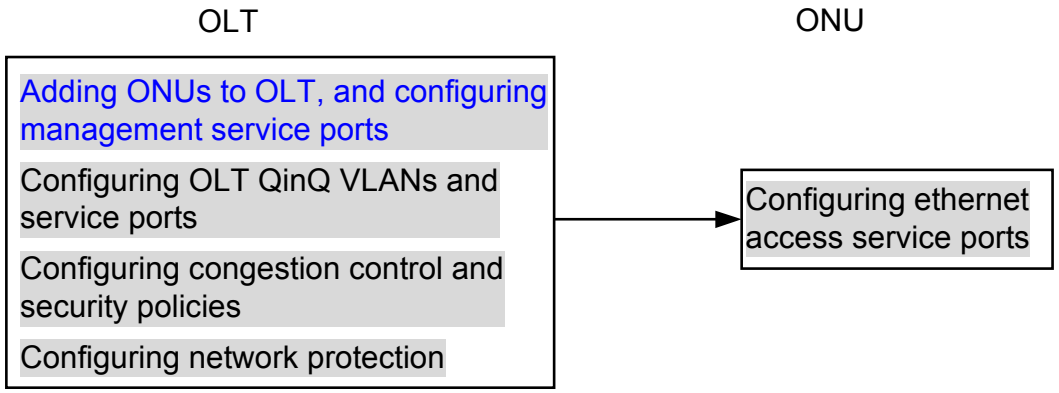
ONU applicable to this scenario: MA5694S

Figure 14-31 Implementing access service of small-cell base stations



14.4.8.2 Configuration Procedure

The following figure shows the configuration procedure for implementing the access service of a small-cell base station (QinQ VLAN and CLI configuration).



14.4.8.3 Configuring Ethernet Access Service Ports on ONUs

Add a service port on an ONU and configure an upstream VLAN to make the ONU-to-user service flows available and create an ONU-to-OLT upstream data channel.

Copyright © Huawei Technologies Co., Ltd.

Data Planning

Configuration Item	Data
Port	Upstream port: 0/0/1 Service port: 0/3/1
SVLAN (upstream VLAN of the ONU)	VLAN for base station access service: ● VLAN for synchronization service: 1000 ● VLAN for OAM service: 1001 ● VLAN for voice and data services: 1002
User VLAN (original VLAN of packets from base stations)	● Synchronization service of base stations: untagged ● VLAN for OAM service of base stations: 20 ● VLAN for voice and data services of base stations: 30
Traffic profile	● ID: 10 ● CIR: OFF ● Priority source: user-cos, default priority: 7 ● Priority policy: tag-in-package

Procedure

Step 1 Create SVLANs and add an upstream port to the VLANs.

Create VLANs 1000, 1001, and 1002.

```
huawei(config)#vlan 1000-1002 smart
huawei(config)#port vlan 1000 0/0 1
huawei(config)#port vlan 1001 0/0 1
huawei(config)#port vlan 1002 0/0 1
```

Step 2 Configure a traffic profile.

Add a traffic profile 10 and do not limit rates. Packets transmitted upstream use the priority (7 by default) copied from the user VLAN. Packets transmitted downstream use the priority carried by themselves.

```
huawei(config)#traffic table ip index 10 cir off priority user-cos 7 priority-policy tag-in-package
```

Step 3 Configure Ethernet access service ports.

Configure service ports for the synchronization service, OAM service, and voice and data services of base stations. According to **14.2.2 Principle of VLAN Data Plan**, ONUs translate user VLANs to a specified CVLAN.

```
huawei(config)#service-port vlan 1000 eth 0/3/1 multi-service user-vlan
 untagged rx-cttr 10 tx-cttr 10  //Syncronization service port
huawei(config)#service-port vlan 1001 eth 0/3/1 multi-service user-vlan
 20 rx-cttr 10 tx-cttr 10  //OAM service port
huawei(config)#service-port vlan 1002 eth 0/3/1 multi-service user-vlan
 30 rx-cttr 10 tx-cttr 10 //Voice and data service port
```


Copyright © Huawei Technologies Co., Ltd.

NOTE

Packets from different base stations may carry different user VLANs. Ensure that user VLANs are consistent with the actual ones during configuration.

----End

14.4.8.4 Configuring Congestion Control and Security Policies

This topic describes how to configure global priority-based scheduling policies for queues to ensure service reliability and configure global security policies to ensure service security.

Context

Congestion control uses queue scheduling technology to map packets sent from the same port into multiple queues and process packets in each queue based on priority. Congestion control is recommended.

Security policies cover system security, user security, and service security, which ensure normal running of services.

NOTE

Enable security features based on service types. For details, see **11.2.7 Principle of Security Data Plan**.

Procedure

- Configure queue scheduling.

  Based on **13.2.3 Principle of QoS Data Plan**, all packets use strict priorities for queue scheduling and are mapped to queues based on priorities.

  ```
  huawei(config)#queue-scheduler strict-priority
  huawei(config)#cos-queue-map cos0 0 cos1 1 cos2 2 cos3 3 cos4 4 cos5 5 cos6 6 cos7 7  //System default
  ```

- Configure system security.
  - Enable deny of service (DoS) anti-attack on both the OLT and optical network units (ONUs).
    1. Run the **security anti-dos enable** command to globally enable DoS anti-attack.
    2. Run the **security anti-dos control-packet policy** command to configure a protocol packet processing policy that will be used when a DoS attack occurs.
    3. Run the **security anti-dos control-packet rate** command to configure the threshold for the rate of sending protocol packets to the CPU.
  - Enable IP address anti-attack on both the OLT and ONUs.

    Run the **security anti-ipattack enable** command to enable IP address anti-attack.
- Configure user security.
  - Enable MAC address anti-flapping on both the OLT and ONUs.

    Run the **security anti-macduplicate enable** command to enable MAC address anti-flapping.

----End

Copyright © Huawei Technologies Co., Ltd.

14.4.8.5 Configuring Clock Synchronization

In this scenario, network-wide clock synchronization is implemented through synchronous Ethernet clocks.

Prerequisites

- The clock daughter board CKMC/CKMD of the SCU board must be in position.
- The ethernet upstream board must be GICK/GSCA (GE port) or X2CS (10GE port)/SPUF (need an independent service board slot).
- The upstream MAN PSN of the OLT must feature the capability of Ethernet synchronization.

Context

The clock synchronization scheme of a small-cell base station can be synchronous Ethernet (frequency synchronization) or IEEE 1588v2 (time synchronization). This topic uses the synchronous Ethernet as an example to describe how to configure clock synchronization. For IEEE 1588v2 time synchronization configurations, see **14.3.6 Configuring 1588v2 Clock Synchronization**.

Data Plan

Configuration Item	Data
GIU upstream board	Port: 0/19/0
DSLAM (MA5616) port	Upstream port: 0/0/1 UNI interface: 0/3/0
ONU Port	Upstream port: 0/0/0 UNI interface: 0/1/0

Procedure

- **Configure the OLT-side clock.**
  1. Configure a system clock source.

     Use the Ethernet line clock input from GIU port 0/19/0 as the system clock. Set the index of the system clock to **0** and priority to **0** (highest priority).

     ```
     huawei(config)#clock source 0 0/19/0
     huawei(config)#clock priority system 0
     ```

  2. Query the configurations and status of the system clock source.

     Run the **display clock source system** command to query the configurations and status of the system clock source. Ensure that the configurations of the system clock source are correct and the status of the system clock source is **Normal**.

     ```
     huawei(config)#display clock source system

     ------------------------------------------------------------------------
     ```


Copyright © Huawei Technologies Co., Ltd.

```
-----
  Index  Board    Source   Clk-type  State       Priority QL
Selected

-------------------------------------------------------------------------
-----
    0    H801GICK 0/19/0    ETH      Normal      0        ---
YES

-------------------------------------------------------------------------
-----
```

Run the **display clock mode** command to query the working mode of the clock. Ensure that the working mode of the clock daughter board is **Tracing**.

```
huawei(config)#display clock mode
  Clock manage-mode:Third-mode
  Clock subboard work-mode:Tracing
```

- **(ONU functioning as the VDSL2 Dock device) Configure the DSLAM-side clock.**

  When the ONU functions as the VDSL2 Dock device, the MA5694S (ONU) is connected upstream to the DSLAM (MA5616) through VDSL2 bonding. In this way, you need to configure clock synchronization on the OLT, DSLAM, and ONU.

  Use the line clock obtained from the upstream port as the system clock.

  ```
  huawei(config)#clock source 0/0/1
  huawei(config)#clock priority system 0
  ```

- **Configure the ONU-side clock.**

  When a small-cell base station is connected to an ONU through the Ethernet port, the port transmit clock is defaulted to the system clock and cannot be modified. Therefore, you need to configure only the system clock of the ONU.

  When the ONU functions as the GPON Dock device, the MA5694S is connected upstream to the OLT through the GPON port. In this way, you need to configure clock synchronization on the OLT and ONU.

  Use the line clock obtained from the upstream port as the system clock.

  1. Use the line clock obtained from the upstream port as the system clock.

     ```
     huawei(config)#clock source 0 0/0/0
     huawei(config)#clock priority system 0
     ```

  2. Query the configurations and status of the system clock source.

     Run the **display clock source** command to query the configurations and status of the system clock source.

     ```
     huawei(config)#display clock source
       ------------------------------------------------------------------------
       Index  Type   Source      State          Priority     QL    Selected
       ------------------------------------------------------------------------
         0    line   0/0/0       Normal           0          ---       YES
         1    --     -/ -/ -     ---              ---        NO        ---
         2    --     -/ -/ -     ---              ---        NO        ---
         3    --     -/ -/ -     ---              ---        NO        ---
         4    --     -/ -/ -     ---              ---        NO        ---
         5    --     -/ -/ -     ---              ---        NO        ---
         6    --     -/ -/ -     ---              ---        NO        ---
         7    --     -/ -/ -     ---              ---        NO        ---
         8    --     -/ -/ -     ---              ---        NO        ---
         9    --     -/ -/ -     ---              ---        NO        ---
       ------------------------------------------------------------------------
     ```

----End

Copyright © Huawei Technologies Co., Ltd.

14.4.8.6 Configuring End to End Protection

The access service of a small-cell base station has high requirements on reliability. Configuring end-to-end (E2E) protection well addresses the requirements.

Context

Configuring upstream and downstream network protection can improve the network reliability. For details, see **13.2.6 Principle of Reliability Data Plan**. Among these reliability configurations:

- The upstream network protection schemes include link aggregation and protection groups. Generally, the link aggregation is configured if the GIU board is used for upstream transmission; the protection group is configured if the control board is used for upstream transmission. Link aggregation and protection group are not configured at the same time.
- The downstream network protection (specifically, type B protection) is intended for service ports.

NOTE

This topic lists several protection schemes supported by the MA5694S. You are advised to choose the proper scheme based on the carriers' requirements and actual network conditions.

Procedure

- Configure link aggregation.

  Create a link aggregation group and add upstream ports 0/19/0 and 0/19/1 to the aggregation group. Each member port in the aggregation group forwards packets based on the source MAC address. The working mode of the aggregation group is LACP static aggregation.

  ```
  huawei(config)#link-aggregation 0/19 0-1 ingress workmode lacp-static
  ```

- Configured a protection group.

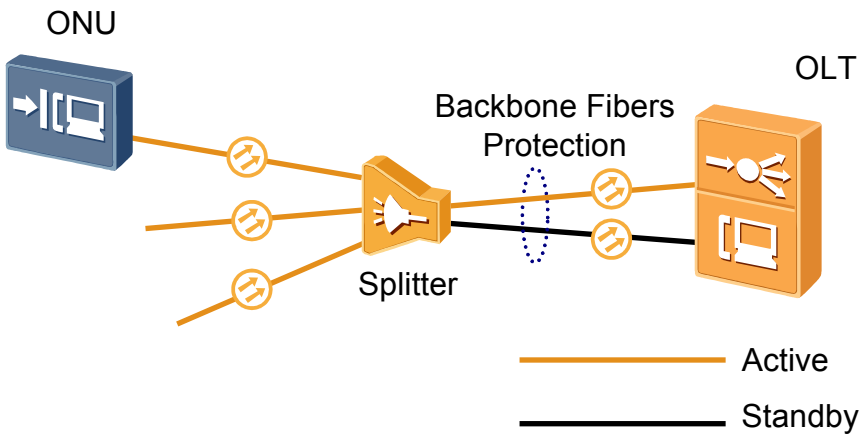
  Create a protection group and add upstream ports 0/19/0 and 0/19/1 on board GIU to the protection group (among which, port 0/19/0 is the working port of the protection group, while port 0/19/1 is the protection port). Set the working mode of the protection group to the delay detection mode, and then enable the protection group.

  ```
  huawei(config-protect)#protect-group first 0/19/0 second 0/19/1 eth workmode timedelay enable
  ```

- Configure type B protection.

  Figure 14-32 shows the example network with type B protection.

  Figure 14-32 Type B network protection



Copyright © Huawei Technologies Co., Ltd.

Create a type B protection group and add ports 0/3/1 and 0/3/2 on the same GPON board of the OLT to the group. Specifically, port 0/3/1 is the working port and port 0/3/2 is the protection port. When port 0/3/1 is faulty, the system can automatically switch services to port 0/3/2 to ensure continued service access.

```
huawei(config)#protect-group 0 protect-target gpon-uni-port workmode timedelay
huawei(protect-group-0)#protect-group member port 0/3/1 role work
huawei(protect-group-0)#protect-group member port 0/3/2 role protect
huawei(protect-group-0)#protect-group enable
```

NOTE

Service configurations on the ONU remain unchanged before and after type B protection is configured. That is, service configurations are applied only to the active GPON port.

----End

14.4.8.7 Verifying Services

The Ethernet base station access service can be verified by checking the connectivity and alarms of the service.

Prerequisites

The base station access service has been deployed.

Procedure

Step 1 Check connectivity.

1. Check the connectivity between base stations and the IP clock server.

   On base stations, configure management IP addresses and static routes to the IP clock server, and then perform ping operations. In normal cases, the ICMP ECHO-REPLY message can be received from the IP clock server.

2. Check the connectivity between base stations and the OAM server.

   On base stations, configure IP addresses of management channels and static routes to the OAM server, and then perform ping operations. In normal cases, the ICMP ECHO-REPLY message can be received from the OAM server.

3. Check the connectivity between base stations and the RNC.

   On base stations, configure service port IP addresses and static routes to the RNC, and then perform ping operations. In normal cases, the ICMP ECHO-REPLY message can be received from the RNC.

Step 2 Check alarms.

Check logs on base stations. Verify that no alarms are generated within 24 hours.

----End

14.4.9 Small-Cell Base Station Access Service (in QinQ VLAN Mode Through GUI Pre-Deployment)

Dock ONUs are connected to small-cell base stations through Ethernet ports, and OLTs interconnect with the devices on the metro network through QinQ VLANs to provide the access service for small-cell base stations. This topic describes how to implement the access service of

Copyright © Huawei Technologies Co., Ltd.

a small-cell base station through GUI pre-deployment in the scenario with the U2000 NMS available.

14.4.9.1 Service Requirements and Application Scenarios

Service Requirements

As the last mile that connects users to the Internet, small-cell backhaul is an important part of an FTTx network. For small-cell backhaul, customers expect to:

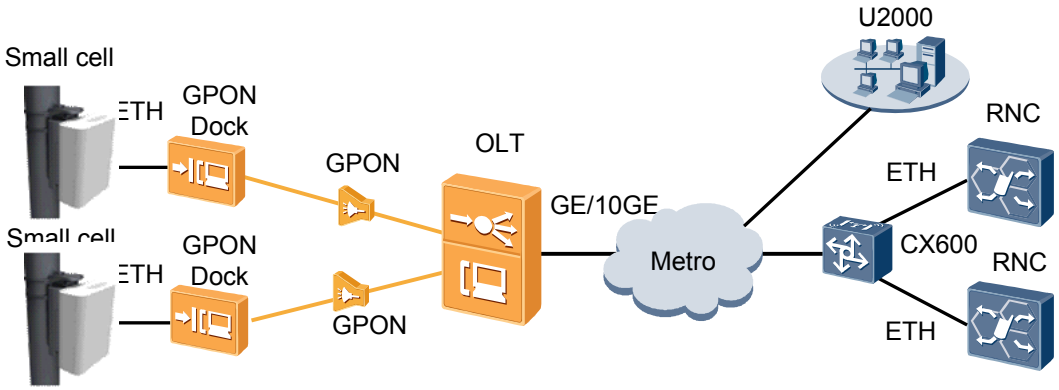
- Make full use of the existing access resources to provide backhaul services for distributed small-cell base stations.
- Use a simple and mature service configuration scheme, featuring a high transmission efficiency in addition to ensuring the QoS.
- Simplify sites to lower the site installation and maintenance costs.

Application Scenarios

As shown in **Figure 14-33**, ONUs, functioning as Dock devices, receive Ethernet service data from small-cell base stations through Ethernet ports and then send the service data to the OLT. The OLT restores the Ethernet signals and adds 2 VLAN tags (QinQ VLAN encapsulation) to the data, so that the data from the small cell bases can be transparently transmitted to the peer PTN devices through the public network and then the PTN devices restore them to the original data.

ONU applicable to this scenario: MA5694S

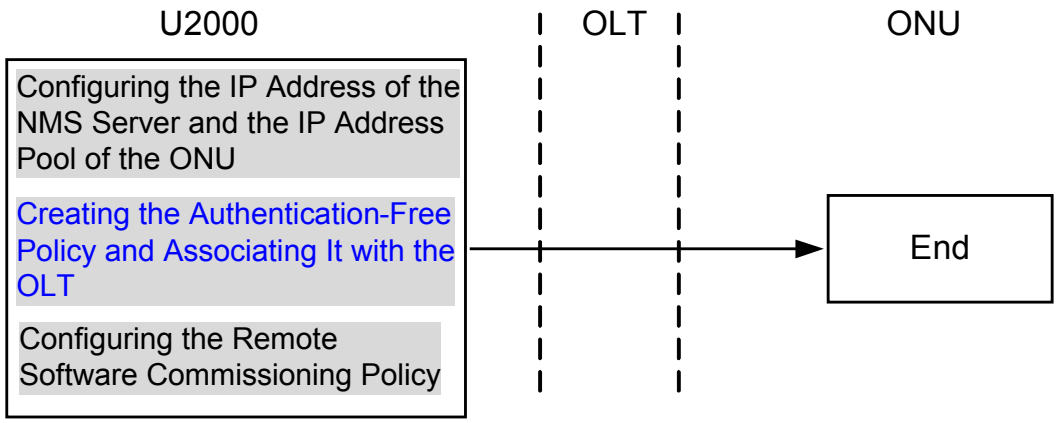
Figure 14-33 Implementing access service of a small-cell base station



14.4.9.2 Configuration Procedure

The following figure shows the configuration procedure for implementing the access service of a small-cell base station (in QinQ VLAN mode through GUI pre-deployment).

Copyright © Huawei Technologies Co., Ltd.



14.4.9.3 Configuring the IP Address of the NMS Server and the IP Address Pool of the ONU (GPON Dock Scenario)

Prerequisites

- The OLT is added to the NMS.
- Related xFTP configurations are completed.

Data Plan

Configuration Item	Data	Remarks
IP address of the NMS server	10.10.10.10	The NMS server needs to use ports 23, 8080, 9801, and 9803. Therefore, ensure that the firewall does not block these ports so that the NMS server can normally communicate with devices.
IP address of the OLT	10.10.10.20	This IP address is designated for Layer 3 VLAN interface 8 and is used for inband management.
IP address pool of the ONU	IP address pool: 10.10.11.2 to 10.10.11.125 Subnet mask: 255.255.254.0 ONU gateway: 10.10.10.20 Management VLAN ID: 8 VLAN priority: 7	The ONU gateway IP address is used as the IP address of the Layer 3 interface on the OLT.

Copyright © Huawei Technologies Co., Ltd.

Procedure

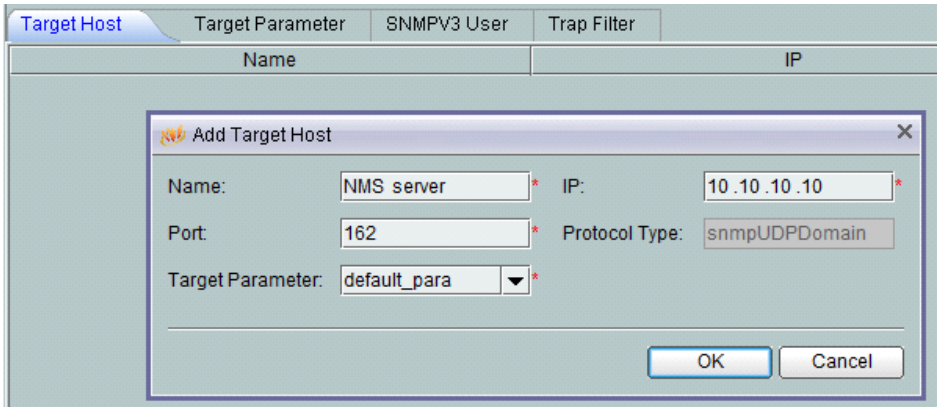
- Configure the IP address of the NMS server used for receiving traps.

  The OLT reports FTTM ONU information to the NMS through traps. Here the trap destination host (namely, the destination host to which traps are sent) is the NMS server.

  For any OLT, only 1 trap destination host is required. If multiple trap destination hosts are configured for the OLT, delete the unnecessary ones.

  1. Choose **Administration** > **NE Communicate Parameter** > **Set NE SNMP Expanded Parameters** (traditional style) from the main menu or select **Fix-Network NE Configuration** in **Application Center** and choose **Administration** > **NE Communicate Parameter** > **Set NE SNMP Expanded Parameters** (application style) from the main menu.
  2. Click **Filter**. In the **Select Device** dialog box, select the desired OLT from the **Device Type** drop-down list and click **OK**.
  3. In the device list, select a record and click the **Target Host** tab.
  4. On the **Target Host** tab, right-click in a blank area and choose **Add** from the shortcut menu.
  5. In the dialog box that is displayed, set the parameters, as shown in **Figure 14-34**.

     Figure 14-34 Configuring the trap destination host

  6. Click **OK**.

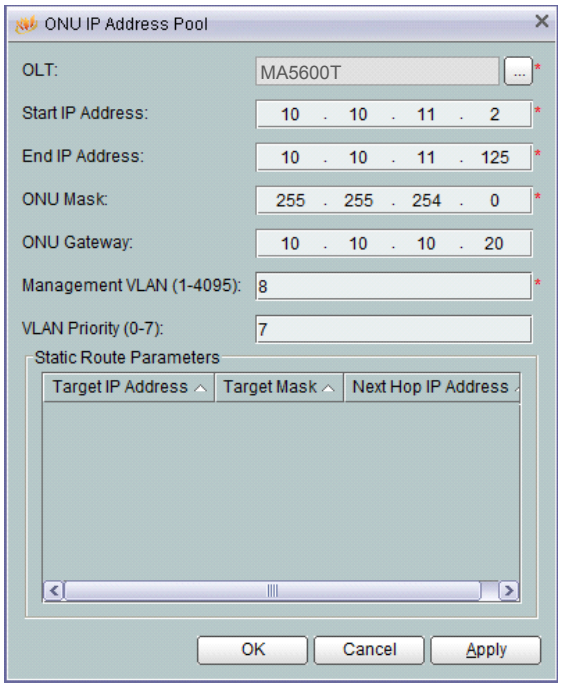
- Configure the IP address pool of the ONU.

  On an FTTM network, IP addresses are automatically allocated because no authentication is required. In this way, an ONU IP address pool needs to be configured so that ONUs, when going online, can automatically obtain an IP address.

  1. Choose **Configuration** > **FTTx Service Pre-Deployment** > **ONU IP Pool Management** (traditional style) from the main menu or select **Fix-Network NE Configuration** in **Application Center** and choose **Access Service** > **FTTx Service Pre-Deployment** > **ONU IP Pool Management** (application style) from the main menu.
  2. In the information list, right-click and choose **Add** from the shortcut menu.
  3. In the dialog box that is displayed, set the parameters, as shown in **Figure 14-35**.

Copyright © Huawei Technologies Co., Ltd.

Figure 14-35 Configuring the IP address pool of the ONU



4. Click **OK**.

----End

14.4.9.4 Creating the Authentication-Free Policy and Associating It with the OLT (GPON Dock Scenario)

Prerequisites

You have completed the configurations of the following profiles:

- SNMP profile
- DBA profile
- Line profile
- MEF IP traffic profile

Context

If you configure an ONU authentication-free policy and associate it with the OLT through the NMS, the FTTM ONU, when going online, will be automatically added to the NMS according to the ONU type and the authentication-free policy.

Data Plan

Configuration Item	Data
SNMP profile	Name: **snmpv1**

Copyright © Huawei Technologies Co., Ltd.

Configuration Item	Data
DBA profile	Name: **MA5694S_dba**
Line profile	Name: **MA5694S_lineprofile**
Management service flow	Name: **pvc_manage**. The attributes of the management service flow are as follows: ● Smart VLAN ID: **8** ● **multi-service user-vlan** (multiple services distinguished by different user VLANs) ● User VLAN ID: **8** ● VLAN translation policy: **translate** ● Upstream and downstream traffic profile: **ip-traffic-table_6**
Voice and data service flow	Name: **pvc_traffic**. The attributes of the voice and data service flow are as follows: ● Smart VLAN ID: **300** ● **multi-service user-vlan** (multiple services distinguished by different user VLANs) ● User VLAN ID: **1002** ● VLAN translation policy: **translate-and-add** ● Upstream and downstream traffic profile: **ip-traffic-table_11**
Base station synchronization service flow	Name: **pvc_sync**. The attributes of the base station synchronization service flow are as follows: ● Smart VLAN ID: **1000** ● **multi-service user-vlan** (multiple services distinguished by different user VLANs) ● User VLAN ID: **1000** ● VLAN translation policy: **transparent** ● Upstream and downstream traffic profile: **ip-traffic-table_10**
Base station OAM service flow	Name: **pvc_oam**. The attributes of the base station OAM service flow are as follows: ● Smart VLAN ID: **300** ● **multi-service user-vlan** (multiple services distinguished by different user VLANs) ● User VLAN ID: **1001** ● VLAN translation policy: **translate-and-add** ● Upstream and downstream traffic profile: **ip-traffic-table_10**

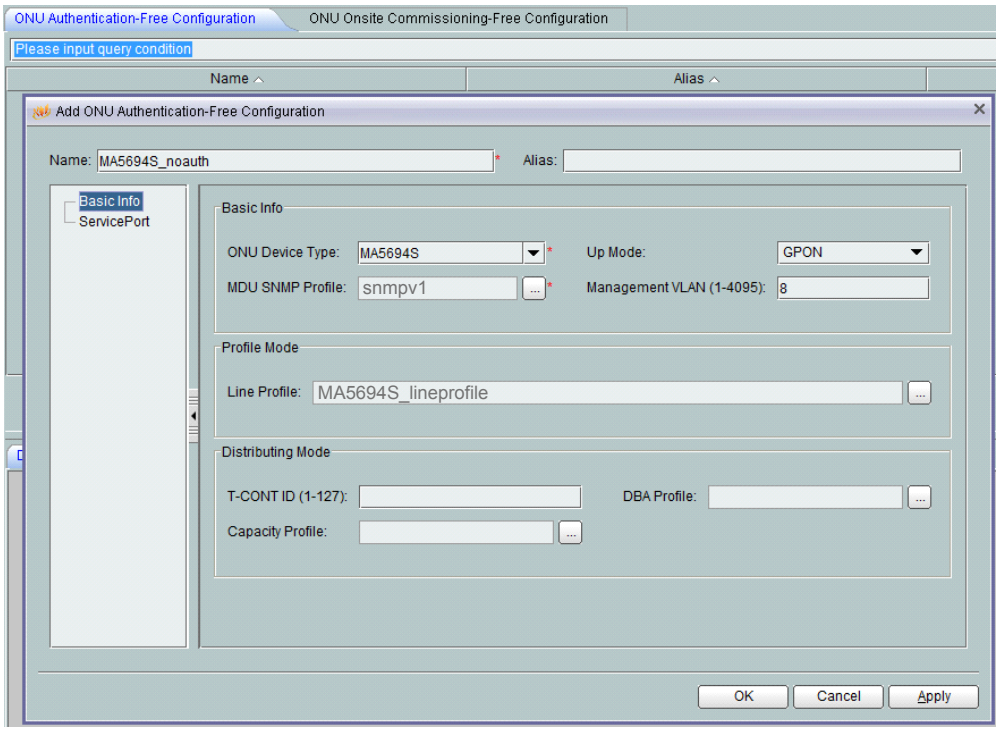
Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Configure the FTTM GPON ONU authentication-free policy.

1. Choose **Configuration** > **FTTx Service Pre-Deployment** > **ONU PnP Management** (compatibility style) from the main menu or select **Fix-Network NE Configuration** in **Application Center** and choose **Access Service** > **FTTx Service Pre-Deployment** > **ONU PnP Management** (application style) from the main menu.
2. Click the **ONU Authentication-Free Configuration** tab.
3. Right-click in a blank area and choose **Add** from the shortcut menu. Configure related parameters in the displayed **Add ONU Authentication-Free Configuration** dialog box, as shown in **Figure 14-36**.

Figure 14-36 Configuring the ONU authentication-free policy



4. Right-click **Service Port** in the navigation tree and choose **Add Service Port** from the shortcut menu to add service ports according to services supported by the small cell.

   Figure 14-37 shows how to add a management service flow; **Figure 14-38** shows how to add a voice and data service flow.

Copyright © Huawei Technologies Co., Ltd.

Figure 14-37 Adding a management service flow

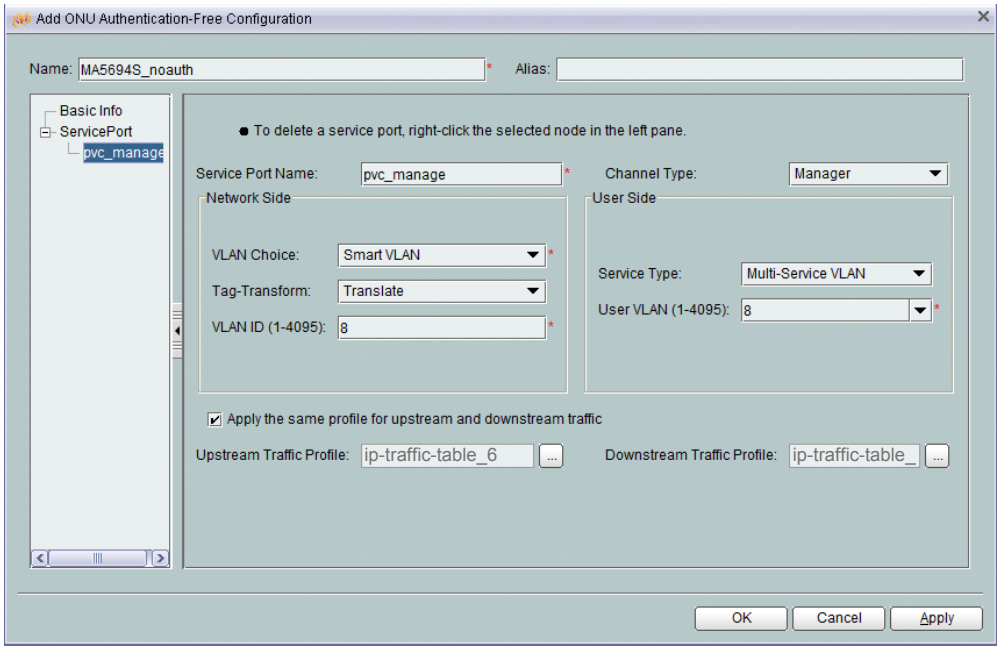
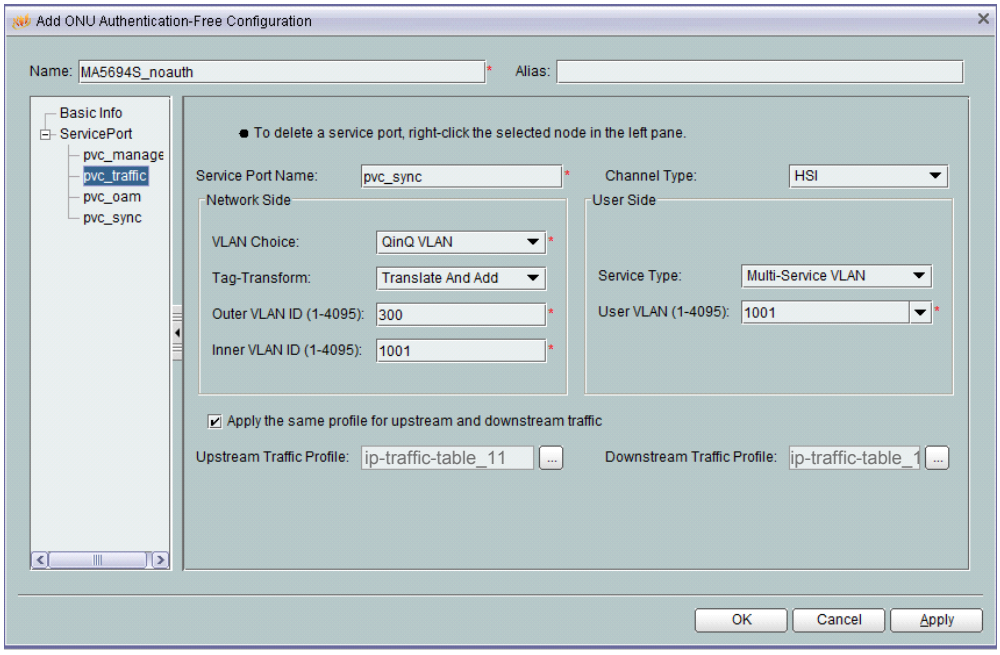


Figure 14-38 Adding a voice and data service flow



Step 2 Associate the ONU authentication-free policy with the OLT.

1. In the authentication-free policy list, select the MDU authentication-free policy and click the **NE Reference** tab in the lower pane.
2. On the **NE Reference** tab, right-click the OLT and choose **Associate** from the shortcut menu.

----End

Copyright © Huawei Technologies Co., Ltd.

14.4.9.5 Configuring the Remote Software Commissioning Policy (GPON Dock Scenario)

Prerequisites

The configuration script is available.

Context

If you configure a remote software commissioning policy through the NMS, the NMS, according to the ONU type and the configured policy, will automatically issue the configuration script to the FTTM ONUs once the ONUs go online, and the service channels will be automatically established.

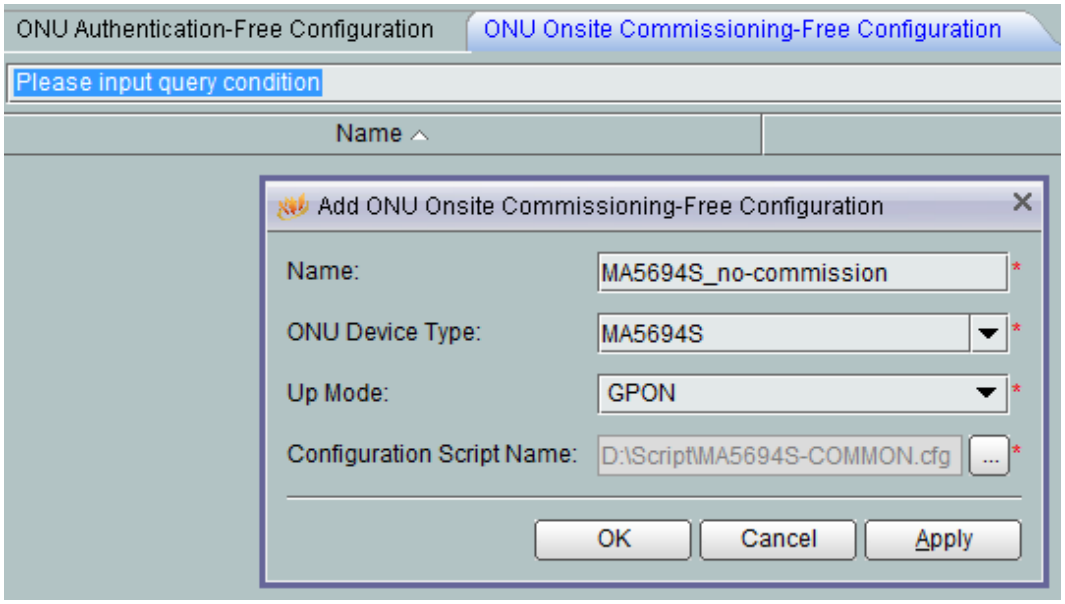
Procedure

Step 1 Choose **Configuration** > **FTTx Service Pre-Deployment** > **ONU PnP Management** (compatibility style) from the main menu or select **Fix-Network NE Configuration** in **Application Center** and choose **Access Service** > **FTTx Service Pre-Deployment** > **ONU PnP Management** (application style) from the main menu.

Step 2 Click the **ONU Onsite Commissioning-Free Configuration** tab.

Step 3 Right-click in a blank area and choose **Add** from the shortcut menu. In the dialog box that is displayed, configure a GPON-upstream MDU commissioning-free policy.

The following figure shows the configuration dialog box.



----End

Copyright © Huawei Technologies Co., Ltd.

14.4.9.6 Configuring Clock Synchronization

In this scenario, network-wide clock synchronization is implemented through synchronous Ethernet clocks.

Prerequisites

- The clock daughter board CKMC/CKMD of the SCU board must be in position.
- The ethernet upstream board must be GICK/GSCA (GE port) or X2CS (10GE port)/SPUF (need an independent service board slot).
- The upstream MAN PSN of the OLT must feature the capability of Ethernet synchronization.

Context

The clock synchronization scheme of a small-cell base station can be synchronous Ethernet (frequency synchronization) or IEEE 1588v2 (time synchronization). This topic uses the synchronous Ethernet as an example to describe how to configure clock synchronization. For IEEE 1588v2 time synchronization configurations, see **14.3.6 Configuring 1588v2 Clock Synchronization**.

Data Plan

Configuration Item	Data
GIU upstream board	Port: 0/19/0
DSLAM (MA5616) port	Upstream port: 0/0/1 UNI interface: 0/3/0
ONU Port	Upstream port: 0/0/0 UNI interface: 0/1/0

Procedure

- **Configure the OLT-side clock.**
  1. Configure a system clock source.

     Use the Ethernet line clock input from GIU port 0/19/0 as the system clock. Set the index of the system clock to **0** and priority to **0** (highest priority).

     ```
     huawei(config)#clock source 0 0/19/0
     huawei(config)#clock priority system 0
     ```

  2. Query the configurations and status of the system clock source.

     Run the **display clock source system** command to query the configurations and status of the system clock source. Ensure that the configurations of the system clock source are correct and the status of the system clock source is **Normal**.

     ```
     huawei(config)#display clock source system

     ------------------------------------------------------------------------
     ```


Copyright © Huawei Technologies Co., Ltd.

```
-----
  Index  Board    Source   Clk-type  State       Priority QL
Selected

-------------------------------------------------------------------------
-----
    0    H801GICK 0/19/0    ETH      Normal      0        ---
YES

-------------------------------------------------------------------------
-----
```

Run the **display clock mode** command to query the working mode of the clock. Ensure that the working mode of the clock daughter board is **Tracing**.

```
huawei(config)#display clock mode
  Clock manage-mode:Third-mode
  Clock subboard work-mode:Tracing
```

- **(ONU functioning as the VDSL2 Dock device) Configure the DSLAM-side clock.**

  When the ONU functions as the VDSL2 Dock device, the MA5694S (ONU) is connected upstream to the DSLAM (MA5616) through VDSL2 bonding. In this way, you need to configure clock synchronization on the OLT, DSLAM, and ONU.

  Use the line clock obtained from the upstream port as the system clock.

  ```
  huawei(config)#clock source 0/0/1
  huawei(config)#clock priority system 0
  ```

- **Configure the ONU-side clock.**

  When a small-cell base station is connected to an ONU through the Ethernet port, the port transmit clock is defaulted to the system clock and cannot be modified. Therefore, you need to configure only the system clock of the ONU.

  When the ONU functions as the GPON Dock device, the MA5694S is connected upstream to the OLT through the GPON port. In this way, you need to configure clock synchronization on the OLT and ONU.

  Use the line clock obtained from the upstream port as the system clock.

  1. Use the line clock obtained from the upstream port as the system clock.

     ```
     huawei(config)#clock source 0 0/0/0
     huawei(config)#clock priority system 0
     ```

  2. Query the configurations and status of the system clock source.

     Run the **display clock source** command to query the configurations and status of the system clock source.

     ```
     huawei(config)#display clock source
       ------------------------------------------------------------------------
       Index  Type   Source      State          Priority     QL    Selected
       ------------------------------------------------------------------------
         0    line   0/0/0       Normal           0          ---       YES
         1    --     -/ -/ -     ---              ---        NO        ---
         2    --     -/ -/ -     ---              ---        NO        ---
         3    --     -/ -/ -     ---              ---        NO        ---
         4    --     -/ -/ -     ---              ---        NO        ---
         5    --     -/ -/ -     ---              ---        NO        ---
         6    --     -/ -/ -     ---              ---        NO        ---
         7    --     -/ -/ -     ---              ---        NO        ---
         8    --     -/ -/ -     ---              ---        NO        ---
         9    --     -/ -/ -     ---              ---        NO        ---
       ------------------------------------------------------------------------
     ```

----End

Copyright © Huawei Technologies Co., Ltd.

14.4.9.7 Verifying Services

The Ethernet base station access service can be verified by checking the connectivity and alarms of the service.

Prerequisites

The base station access service has been deployed.

Procedure

Step 1 Check connectivity.

1. Check the connectivity between base stations and the IP clock server.

   On base stations, configure management IP addresses and static routes to the IP clock server, and then perform ping operations. In normal cases, the ICMP ECHO-REPLY message can be received from the IP clock server.

2. Check the connectivity between base stations and the OAM server.

   On base stations, configure IP addresses of management channels and static routes to the OAM server, and then perform ping operations. In normal cases, the ICMP ECHO-REPLY message can be received from the OAM server.

3. Check the connectivity between base stations and the RNC.

   On base stations, configure service port IP addresses and static routes to the RNC, and then perform ping operations. In normal cases, the ICMP ECHO-REPLY message can be received from the RNC.

Step 2 Check alarms.

Check logs on base stations. Verify that no alarms are generated within 24 hours.

----End

Copyright © Huawei Technologies Co., Ltd.

15 OptiCable D-CMTS Configuration (MA5633 Working as a Remote Extended Frame)

About This Chapter

The OptiCable solution implements cable TV (CATV) and broadband signal transmission over a coaxial network. It applies in CATV network reconstruction in upstream and downstream directions or new residential areas requiring the CATV and broadband services over a coaxial network. The radio frequency (RF) access mode applies in the PON+distributed cable modem termination system (D-CMTS) scenario. This mode complies with the data over cable service interface specification (DOCSIS) and supports multiple broadcast and TV services, such as high-speed Internet (HSI) and IPTV services. The OptiCable centralized management solution, in which an MA5633 works as a remote extended frame of an optical line terminal (OLT), supports more D-CMTSs without increasing the number of management IP addresses, thereby simplifying D-CMTS management and reducing maintenance costs.

15.1 D-CMTS Service Overview
This section describes the services supported by a distributed cable modem termination system (D-CMTS) for multiservice operators (MSOs) from the aspect of basic concepts, networking scenarios, and hardware configurations. This information provides a basis for configuring the services on the D-CMTS.

15.2 Data Plan Principles for D-CMTS Services
This section describes the principles of planning frequency spectrum management, device management, quality of service (QoS), and VLANs for distributed cable modem termination system (D-CMTS) services.

15.3 Service Configuration on a D-CMTS That Works as a GPON Remote Extended Frame on a Layer 3 Network
This section describes how to configure services, including home services, L2VPN enterprise service, and wireless local area network (WLAN) hotspot radio backhaul service, on an optical line terminal (OLT) when a distributed cable modem termination system (D-CMTS) works as a GPON extended frame on a Layer 3 network. The MA5603T equipped with the SCUV, GPMD, and SPUF boards is used as an example.

15.4 Service Configuration on a D-CMTS That Works as a GE Remote Extended Frame on a Layer 3 Network

Copyright © Huawei Technologies Co., Ltd.

This section describes how to configure services, including the Internet access service, voice service, and VoD service, on an optical line terminal (OLT) when a distributed cable modem termination system (D-CMTS) works as a GE remote extended frame on a Layer 3 network. The MA5603T equipped with the SCUV, ETHB, and SPUF boards is used as an example.

15.5 Service Configuration on a D-CMTS That Works as a GPON Remote Extended Frame on a Layer 2 Telecom Network

This section describes how to configure services, including home services, L2VPN enterprise service, and wireless local area network (WLAN) hotspot radio backhaul service, on an optical line terminal (OLT) when a distributed cable modem termination system (D-CMTS) works as a GPON extended frame on a Layer 2 telecom network. The MA5603T equipped with the SCUV, GPMD, and SPUF boards is used as an example.

Copyright © Huawei Technologies Co., Ltd.

15.1 D-CMTS Service Overview

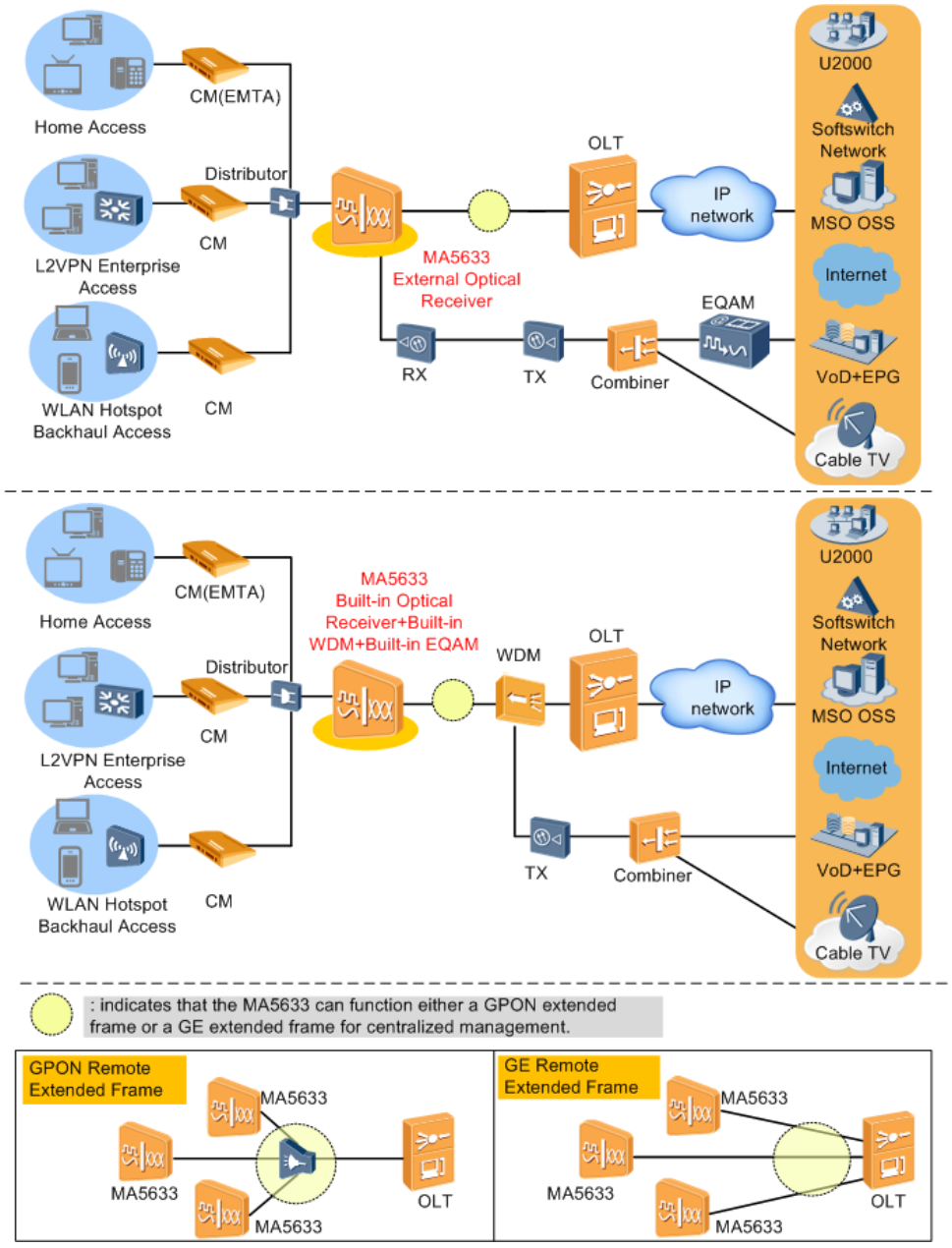
This section describes the services supported by a distributed cable modem termination system (D-CMTS) for multiservice operators (MSOs) from the aspect of basic concepts, networking scenarios, and hardware configurations. This information provides a basis for configuring the services on the D-CMTS.

15.1.1 Basic Concepts

This section describes basic concepts related to a distributed cable modem termination system (D-CMTS) from the user side to the network side on D-CMTS networks when the MA5633 works as a GPON or GE remote extended frame.

Copyright © Huawei Technologies Co., Ltd.

Figure 15-1 D-CMTS networking when the MA5633 works as an extended frame



User Home Side

Concept	Description
Cable modem (CM)	A device that connects customer premises equipment (CPE) to a hybrid fiber coaxial (HFC) network. It transmits data over a cable network through data over cable service interface specification (DOCSIS).

Copyright © Huawei Technologies Co., Ltd.

Concept	Description
Media terminal adapter (MTA)	A network client that provides user terminal (such as a phone set)-oriented ports and call control unit-oriented network signaling interfaces. It connects to cable network units through an HFC network. MTAs are classified into embedded MTAs (EMTAs) and single MTAs (SMTAs) according to PacketCable. ● An EMTA integrates CM and MTA functions. ● An SMTA supports only MTA functionalities.
VoD	A technology that enables users to order any program in a VoD program library. During program playing, users can perform operations, such as pause, fast forward, fast rewind, and program locating.
Distributor	A component that distributes signals in a cable TV (CATV) transmission system. It equally outputs several channels of signals from one channel of input signals. The common distribution ratios are 1:2, 1:3, 1:4, and 1:6.

Optical Node

Concept	Description
D-CMTS	A device that connects an aggregation network to an HFC network. It forwards network data, processes protocols, and modulates or demodulates radio frequency (RF) signals. The D-CMTS provides the quality of service (QoS) required by CMs and allocates upstream bandwidths and service resources to the CMs based on CMs' request and network QoS policy.
Built-in optical receiver	● An optical receiver, which performs optical-to-electrical (O/E) conversion for CATV and upstream backhaul signals. ● The fiber node does not require an additional optical receiver. The O/E conversion is performed by the optical receiver built in the MA5633 and the MA5633 can receive CATV optical signals.
Built-in WDM	● A device that multiplexes the optical signals with different standard wavelengths into one channel of multiplexed signals and transmits the signals over one optical fiber. ● The WDM in the branch equipment room combines data signals and CATV signals for signal transmission over one feeder fiber. On the optical node, the WDM built in the MA5633 separates the two types of signals from each other.

Copyright © Huawei Technologies Co., Ltd.

Concept	Description
Built-in EQAM	● The edge quadrature amplitude modulation (EQAM) feature enables the MA5633 to function as the gateway of a hybrid fiber coaxial (HFC) network connected to an IP network. The MA5633 multiplexes and modulates IP signals into radio frequency (RF) signals so that the data carried in the IP signals can be transmitted over the HFC network. ● The EQAM built in the MA5633 is moved downwards from the branch equipment room to the fiber node. Therefore, the fiber node does not require an additional EQAM. ● Video streams are transmitted over a MAN network through the OLT to the MA5633. The MA5633 uses the built-in EQAM to module the video signals into RF signals and sends the RF signals to the STB.
Splitter	A component that connects to the center of a branch or feeder fiber. It consists of a main input end, a main output end, and multiple branch output ends. Each branch output end receives only few input signals on the main path. The majority signals are transmitted forward over the main path.

Branch Equipment Room

Concept	Description
PON	A passive optical network (PON) uses a point-to-multipoint (P2MP) network architecture. A PON network consists of three parts: optical line terminal (OLT), optical distribution network (ODN), and optical network units (ONUs). A PON network uses optical fibers for data transmission, supports more users with less optical fiber resources, and provides a higher access rate. Mainstream PON technologies include broadband passive optical network (BPON), Ethernet passive optical network (EPON), and gigabit passive optical network (GPON).
Optical distribution network (ODN)	A network that is composed of passive optical components, such as optical fibers and one or more passive optical splitters. The ODN provides highly reliable optical channels between the OLT and ONUs.
Optical line terminal (OLT)	An aggregation device located at the central office (CO), which terminates PON protocols.
Optical splitter	A passive component, which allocates optical power to multiple ONUs connected to one feeder fiber. In a GPON network that consists of an OLT, ONUs, optical splitters, and optical fibers, the optical fiber connected to the OLT uses an optical splitter to connect to multiple ONUs. The number of ONUs that can be connected to the optical fiber is determined based on the split ratio.

Copyright © Huawei Technologies Co., Ltd.

Concept	Description
RX	An optical receiver, which performs optical-to-electrical (O/E) conversion for CATV and upstream backhaul signals.
TX	An optical transmitter, which performs O/E conversion for received CATV signals.
Combiner	A component that combines multiple channels of analog signals into one channel of signals on an RF port and then sends the signals to the downstream optical TX.
GPON remote extended frame	An OLT, deployed in a branch equipment room and working as a main frame, connects to an MA5633 through a GPON cascading board. In this manner, the MA5633 is no longer a standalone NE (no longer allocated with an independent management IP address), but is managed by the OLT. The MA5633 is regarded as a remote service board of the OLT and has the same functions and features as those of the OLT.
GE remote extended frame	An OLT, deployed in a branch equipment room and working as a main frame, connects to an MA5633 through a GE cascading board. In this manner, the MA5633 is no longer a standalone NE (no longer allocated with an independent management IP address), but is managed by the OLT. The MA5633 is regarded as a remote service board of the OLT and has the same functions and features as those of the OLT. **NOTE** The difference between a GPON remote extended frame and a GE remote extended frame lies in transmission media and network structure. Specifically, the networking for the GPON remote extended frame is of the point-to-multipoint (P2MP) structure and that for the GE remote extended frame is of the point-to-point (P2P) structure.

MAN Network

Concept	Description
Softswitch or IP multimedia subsystem (IMS)	Softswitch: core of the NGN network call and control, which supports call and connection control for the services having high real-time requirements. For the softswitch, services are separated from call control and call control is separated from bearing. In addition, the softswitch uses open service interface (API) and standard protocols, which facilitates the development for new services and features. IMS: uses Session Initiation Protocol (SIP) signaling as the call control signaling. It provides voice, data, and multimedia services.
Broadband TV (BTV) source	IPTV head end, a contents preparation platform in the IPTV system. It receives signals, converts media formats, and manages media materials.

Copyright © Huawei Technologies Co., Ltd.

15.1.2 Networking Scenarios and Hardware Configurations (GPON)

This section describes networking scenarios of a distributed cable modem termination system (D-CMTS) when the D-CMTS works as a GPON remote extended frame and D-CMTS's hardware configurations.

Networking Scenarios and Hardware Configurations

Networking Scenario	Description	OLT Device	ONU Device
Home service networking	In home service networking, a distributed cable modem termination system (D-CMTS) connects to cable modems (CMs) at user homes through radio frequency (RF) ports and provides home services for users, including the cable TV (CATV) service, Internet access service, VoD service, broadband TV (BTV) service, and PacketCable service.	● MA5603T or MA5600T: – Control board: SCUV – Service board: GPMD – Upstream interface board: SPUF ● MA5608T: – Control board: MCUE – Service board: GPMD	MA5633
L2VPN enterprise service networking	In L2VPN enterprise service networking, a distributed cable modem termination system (D-CMTS) connects to cable modems (CMs) through radio frequency (RF) ports, and the CMs connect to switches or routers to provide the L2VPN service for users.		
Wireless local area network (WLAN) hotspot radio backhaul service networking	In wireless local area network (WLAN) hotspot radio backhaul service networking, a distributed cable modem termination system (D-CMTS) connects to cable modems (CMs) through radio frequency (RF) ports. A CM connects to wireless access points (APs) to provide wireless fidelity (Wi-Fi) access for users.		

Copyright © Huawei Technologies Co., Ltd.

15.1.3 Networking Scenarios and Hardware Configurations (GE)

This section describes networking scenarios of a distributed cable modem termination system (D-CMTS) when the D-CMTS works as a GE remote extended frame and D-CMTS's hardware configurations.

Networking Scenarios and Hardware Configurations

Networking Scenario	Description	OLT Device	ONU Device
Home service networking	In home service networking, a distributed cable modem termination system (D-CMTS) connects to cable modems (CMs) at user homes through radio frequency (RF) ports and provides home services for users, including the cable TV (CATV) service, Internet access service, VoD service, broadband TV (BTV) service, and PacketCable service.	● MA5603T or MA5600T: – Control board: SCUV – Service board: ETHB – Upstream interface board: SPUF ● MA5608T: – Control board: MCUE – Service board: ETHB	MA5633
L2VPN enterprise service networking	In L2VPN enterprise service networking, a distributed cable modem termination system (D-CMTS) connects to cable modems (CMs) through radio frequency (RF) ports, and the CMs connect to switches or routers to provide the L2VPN service for users.		
Wireless local area network (WLAN) hotspot radio backhaul service networking	In wireless local area network (WLAN) hotspot radio backhaul service networking, a distributed cable modem termination system (D-CMTS) connects to cable modems (CMs) through radio frequency (RF) ports. A CM connects to wireless access points (APs) to provide wireless fidelity (Wi-Fi) access for users.		

Copyright © Huawei Technologies Co., Ltd.

15.2 Data Plan Principles for D-CMTS Services

This section describes the principles of planning frequency spectrum management, device management, quality of service (QoS), and VLANs for distributed cable modem termination system (D-CMTS) services.

15.2.1 Frequency Spectrum Management

Total Frequency Bandwidth

The total frequency bandwidth supported by a distributed cable modem termination system (D-CMTS) ranges from 5 MHz to 1 GHz.

Upstream Frequency Bandwidth

The upstream frequency bandwidth supported by a D-CMTS can be of the European or North American standard.

- European standard: 5 MHz to 65 MHz
- North American standard: 5 MHz to 42 MHz

Downstream Frequency Bandwidth

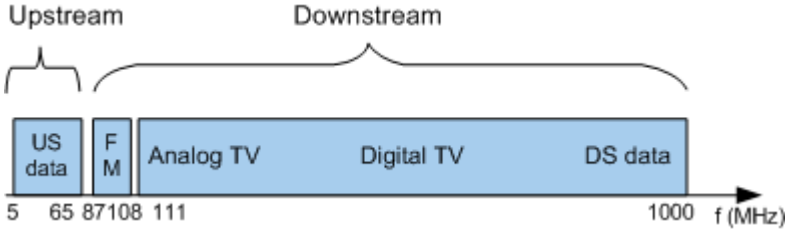
The downstream frequency bandwidth supported by a D-CMTS can be of the European or North American standard.

- European standard: 87 MHz to 1002 MHz
- North American standard: 57 MHz to 1002 MHz

Recommended Frequency Spectrum Configuration

Figure 15-2 lists the recommended frequency spectrum configuration, using the European standard as an example.

Figure 15-2 Recommended frequency spectrum configuration



Copyright © Huawei Technologies Co., Ltd.

Table 15-1 Description of recommended frequency spectrum configuration

Item	Planning Suggestion	Planning Principle
Upstream frequency bandwidth	The upstream frequency bandwidth ranging from 5 MHz to 15 MHz is used to transmit low-traffic data without strict requirements on signal-to-noise ratio (SNR), such as network status monitoring, VoD, user passwords, and program indexes.	● Plan the upstream frequency bandwidth for the cable TV (CATV) service to support the services that have been provisioned and those to be provisioned. ● Plan continuous upstream frequency bandwidths for the analog TV service, digital TV service, and data over cable service interface specification (DOCSIS) data service to prevent interference between the services. In addition, the planning should facilitate the system in handling the issues of a service without affecting other services.
	The upstream frequency bandwidth ranging from 16 MHz to 65 MHz is used to transmit upstream data.	
Downstream frequency bandwidth	The downstream frequency bandwidth ranging from 87 MHz to 108 MHz is used to carry the frequency modulation (FM) broadcast service. The FM frequency is 400 kHz. The downstream frequency bandwidth supports 52 frequency points.	
	The downstream frequency bandwidth ranging from 111 MHz to 1 GHz is used to carry the analog TV service, digital service, and DOCSIS data service. In the range from 111 MHz to 1 GHz: ● 111 MHz to 550 MHz: analog TV service ● 550 MHz to 750 MHz: digital TV service ● 750 MHz to 1 GHz: DOCSIS data service	

Copyright © Huawei Technologies Co., Ltd.

15.2.2 Device Management

Data Plan for Device Management

Item	Device or Service	Planning Principle
Management channel	Optical line terminal (OLT)	The management VLANs of all OLTs on an entire network carry only service VLAN tags.
IP address	Device management	The management IP address of an OLT uses a private IP address to ensure the OLT security.
	Cable modem (CM)	A CM obtains a private IP address through Dynamic Host Configuration Protocol (DHCP).
	Internet access service	The high-speed Internet (HSI) service uses public IP addresses, which are planned by carriers.
	PacketCable service	A media terminal adapter (MTA) obtains a private IP address through DHCP.
	VoD and multicast services	A set top box (STB) obtains a private IP address through DHCP for program ordering.

15.2.3 QoS

Quality of service (QoS) planning varies according to service types. For details, see **Table 15-2**.

Service Priority Planning and Queue Scheduling Policy

Table 15-2 Service priority planning and queue scheduling policy

Service Type	802.1p	Queue
Network protocol and signaling	6	CS6 (PQ)
VoIP	5	EF (PQ)
IPTV, OAM for EMS or NMS, and golden enterprises	4	AF4 (WFQ)
Silver enterprise	3	AF3 (WFQ)
Bronze enterprise	2	AF2 (WFQ)
High-speed Internet (HSI) service	0	BE (WFQ)

Copyright © Huawei Technologies Co., Ltd.

NOTE

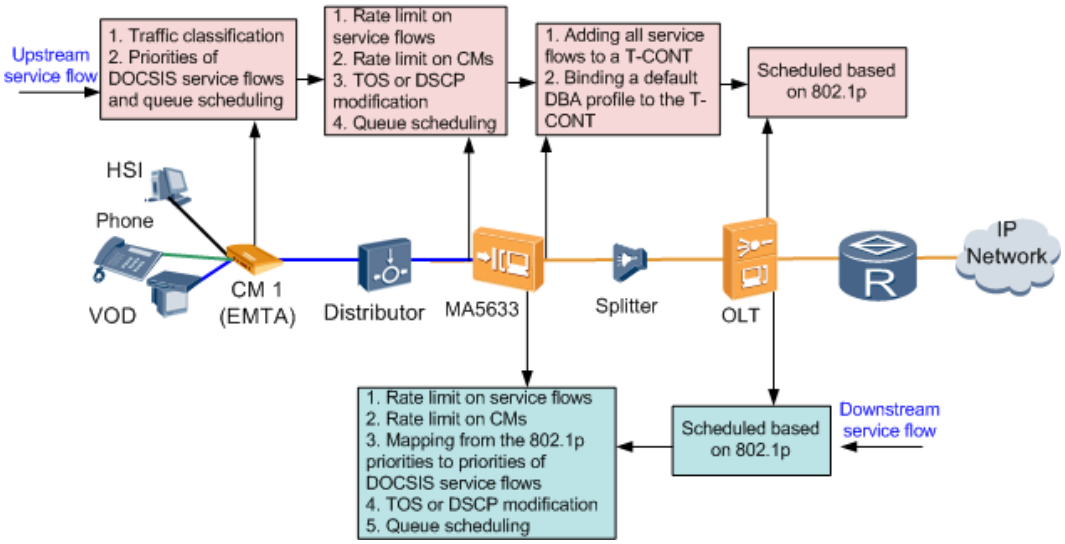
The priorities listed in the preceding table are recommended. Change the priorities based on site and carriers' requirements.

QoS Model

Figure 15-3 shows the end to end (E2E) QoS processing for the data over cable service interface specification (DOCSIS) service. This section uses a distributed cable modem termination system (D-CMTS) that works as a GPON remote extended frame of an optical line terminal (OLT) as an example.

The only difference between the QoS processing for a D-CMTS that works as a GE extended frame and that for a D-CMTS that works as a GPON extended frame is as follows: The QoS processing is not required for the GPON module of the D-CMTS that works as a GE extended frame.

Figure 15-3 QoS module for a D-CMTS that works as a GPON extended frame



Copyright © Huawei Technologies Co., Ltd.

Table 15-3 QoS planning principles

Service	Packet Direction	QoS Planning		
		CM	D-CMTS	OLT
Cable modem (CM) control service, HSI service, or VoIP service	Upstream	1. A CM classifies flows for service packets. 2. A CM schedules queues according to the priorities of DOCSIS service flows.	● Coaxial media converter (CMC) module QoS parameters are defined in a CM configuration file. Using the QoS parameter settings, a D-CMTS limits service rates or schedules queues by priorities. In addition, an OLT supports the configuration of a QoS profile, which defines QoS parameters for various CM services. If a QoS parameter is defined both in a CM configuration file and a QoS profile, the configuration in the CM configuration file preferentially takes effect. 1. A D-CMTS limits CM service rates based on service priority. 2. A D-CMTS limits the rate of a CM service flow group. 3. A D-CMTS schedules queues for service flows. ● GPON module	An OLT maps the priority of a DOCSIS service flow to the 802.1p field in the Ethernet header and uses the 802.1p priority to schedule queues.

Copyright © Huawei Technologies Co., Ltd.

Service	Packet Direction	QoS Planning		
		CM	D-CMTS	OLT
			1. All service flows are mapped from GPON encapsulation mode (GEM) port 0 to transmission container (T-CONT) 1. 2. T-CONT 1 is bound to the default dynamic bandwidth allocation (DBA) profile. T-CONT 1 is of type 4 and supports a maximum bandwidth of 1000 Mbit/s.	
	Downstream	A CM does not control traffic.	A D-CMTS controls traffic based on traffic settings of DOCSIS service flows and performs committed access rate (CAR) based on the CM traffic control parameters defined in a CM configuration file.	An OLT uses the 802.1p priority to schedule queues.
L2VPN enterprise or wireless local area network (WLAN) hotspot radio backhaul service	The QoS processing for L2VPN enterprise and WLAN hotspot radio backhaul services is the same as that for home services.			

Copyright © Huawei Technologies Co., Ltd.

15.2.4 VLAN

Table 15-4 VLAN planning principles

Service	VLAN Tag Translation		
	CM	**OLT (Main Frame)**	**Layer 3 MAN Device**
Internet access service	The packets of the Internet access service do not carry a VLAN tag. A service flow is created between a cable modem (CM) and a distributed cable modem termination system (D-CMTS).	CM management packets and high-speed Internet (HSI) packets carry the same VLAN tag. ● When an OLT forwards services at Layer 2, the OLT transparently transmits VLAN tags to a MAN device. ● When an OLT forwards services at Layer 3, the OLT adds a unique VLAN tag to the packets of a service type.	● When an OLT forwards services at Layer 2, a Layer 3 MAN device forwards the services at Layer 3 and adds a unique VLAN tag to the packets of a service type. ● When an OLT forwards services at Layer 3, a Layer 3 MAN device forwards the services at Layer 3.
VoD service	The packets of the VoD service do not carry a VLAN tag. A service flow is created between a CM and a D-CMTS.	CM management packets and electronic program guide (EPG) packets carry the same VLAN tag. ● When an OLT forwards services at Layer 2, the OLT transparently transmits VLAN tags to a MAN device. ● When an OLT forwards services at Layer 3, the OLT adds a unique VLAN tag to the packets of a service type.	● When an OLT forwards services at Layer 2, a Layer 3 MAN device forwards the services at Layer 3 and adds a unique VLAN tag to the packets of a service type. ● When an OLT forwards services at Layer 3, a Layer 3 MAN device forwards the services at Layer 3.

Copyright © Huawei Technologies Co., Ltd.

Service	VLAN Tag Translation		
	CM	OLT (Main Frame)	Layer 3 MAN Device
VoIP service	The packets of the VoIP service do not carry a VLAN tag. A service flow is created between a CM and a D-CMTS.	CM management packets and VoIP packets carry the same VLAN tag. ● When an OLT forwards services at Layer 2, the OLT transparently transmits VLAN tags to a MAN device. ● When an OLT forwards services at Layer 3, the OLT adds a unique VLAN tag to the packets of a service type.	● When an OLT forwards services at Layer 2, a Layer 3 MAN device forwards the services at Layer 3 and adds a unique VLAN tag to the packets of a service type. ● When an OLT forwards services at Layer 3, a Layer 3 MAN device forwards the services at Layer 3.
L2VPN enterprise service	The packets of the L2VPN enterprise service do not carry a VLAN tag. Two service flows are created between a CM and a D-CMTS. One is the default service flow and the other is the VPN service flow.	CM management packets and enterprise packets carry different VLAN tags. The VLAN pre-configured for the packets of the L2VPN enterprise service must be the same as that configured in the CM configuration file. ● When an OLT forwards services at Layer 2, the OLT transparently transmits VLAN tags to a MAN device. ● When an OLT forwards services at Layer 3, the OLT adds a unique VLAN tag to the packets of a service type.	● When an OLT forwards services at Layer 2, a Layer 3 MAN device forwards the services at Layer 3 and adds a unique VLAN tag to the packets of a service type. ● When an OLT forwards services at Layer 3, a Layer 3 MAN device forwards the services at Layer 3.

Copyright © Huawei Technologies Co., Ltd.

Service	VLAN Tag Translation		
	CM	OLT (Main Frame)	Layer 3 MAN Device
Wireless local area network (WLAN) hotspot radio backhaul service	The packets of the WLAN hotspot radio backhaul service do not carry a VLAN tag. Two service flows are created between a CM and a D-CMTS. One is the default service flow and the other is the Wi-Fi service flow.	CM management packets and Wi-Fi packets carry different VLAN tags. The VLAN pre-configured for the Wi-Fi packets must be the same as that configured in the CM configuration file. ● When an OLT forwards services at Layer 2, the OLT transparently transmits VLAN tags to a MAN device. ● When an OLT forwards services at Layer 3, the OLT adds a unique VLAN tag to the packets of a service type.	● When an OLT forwards services at Layer 2, a Layer 3 MAN device forwards the services at Layer 3 and adds a unique VLAN tag to the packets of a service type. ● When an OLT forwards services at Layer 3, a Layer 3 MAN device forwards the services at Layer 3.

The VLAN planning principles are summarized as follows:

- HSI, VoIP, and CM management services for home users carry the same S-VLAN tag on a layer 3 network.
- HSI, VoIP, and CM management services for home users carry the different S-VLAN tags on a layer 2 telecom network. Service types can be identified based on VLANs.
- An OLT identifies the L2VPN enterprise and WLAN hotspot radio backhaul services by S-VLAN tag.

  NOTE

  When planning a VLAN, ensure that the VLAN for the L2VPN service is different from S-VLANs.

15.2.5 VLAN Planning for Telecom Networks

Overview

With the development of hybrid fiber coaxial networks, CMTSs are evolving from traditional CMTSs to coaxial media converters (CMCs) and the deployment location has been moved downwards from distribution hubs to fiber nodes. In this case, the application of the CMTSs on traditional telecom networks poses the following challenges:

- The number of access network layers is changed from two to five. Specifically, the original layers CMTSs and cable modems (CMs) are enlarged to routers, convergence LAN

Copyright © Huawei Technologies Co., Ltd.

switches, CMCs, CMs, and home gateways (HGWs). The enlarged Layer 2 network promotes higher requirements on the CMCs for processing VLANs.

- Some carriers deploy HGWs on the lower-layer of CMs. The HGWs add different VLAN tags to packets based on service types. This requires that the CMCs support transparent transmission of VLAN tags.

Values

VLAN classification based on service types on traditional telecom networks brings the following business value points for carriers:

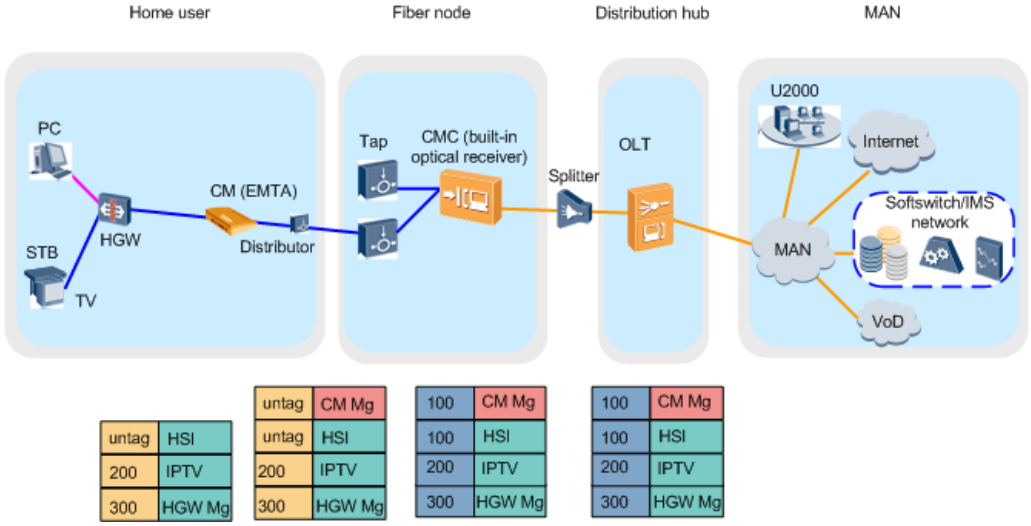
- Services are isolated, which narrows down the broadcast scope.
- Service types can be identified based on VLANs.
- Layer 2 networks can be managed based on VLANs.
- Forwarding paths can be selected on Layer 2 networks based on VLANs.

Typical Network Planning

NOTE

The VLAN tags used in the following section are for reference only.

Figure 15-4 VLAN tag transparent transmission (home access)

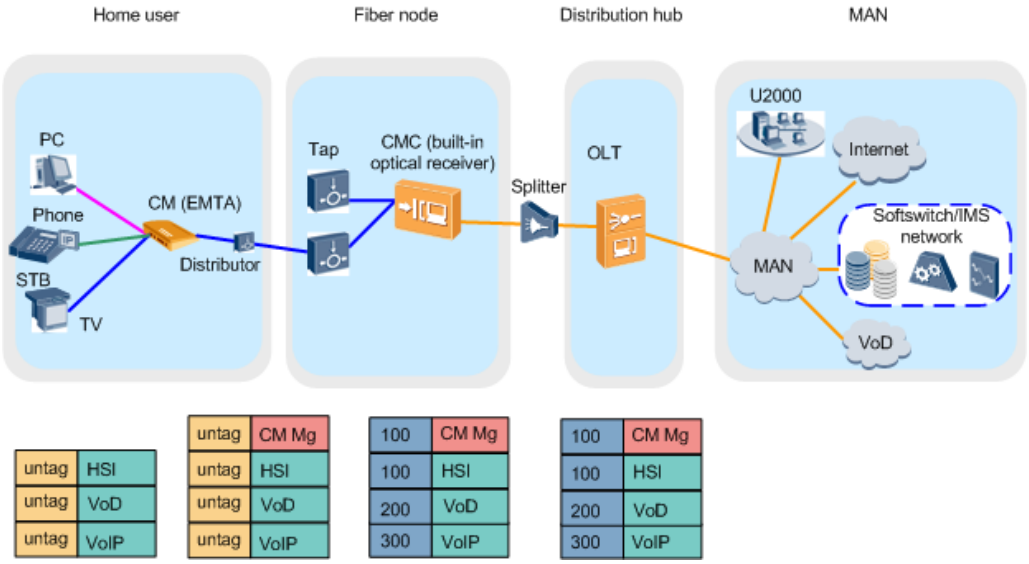


In the preceding network, IP addresses are allocated and service flows and VLAN tags are processed as follows:

1. The PC, set top box (STB), HGW, and CM use dynamic IP addresses allocated by a Dynamic Host Configuration Protocol (DHCP) server.
2. All packets sent by the PC and STB are untagged. The HGW adds VLAN tag 200 to STB packets, adds VLAN tag 300 to HGW management packets (HGW Mg), and transparently transmits high-speed Internet (HSI) service packets.
3. The CMC adds VLAN tag 100 to the HSI service packets and CM management packets (CM Mg).

Copyright © Huawei Technologies Co., Ltd.

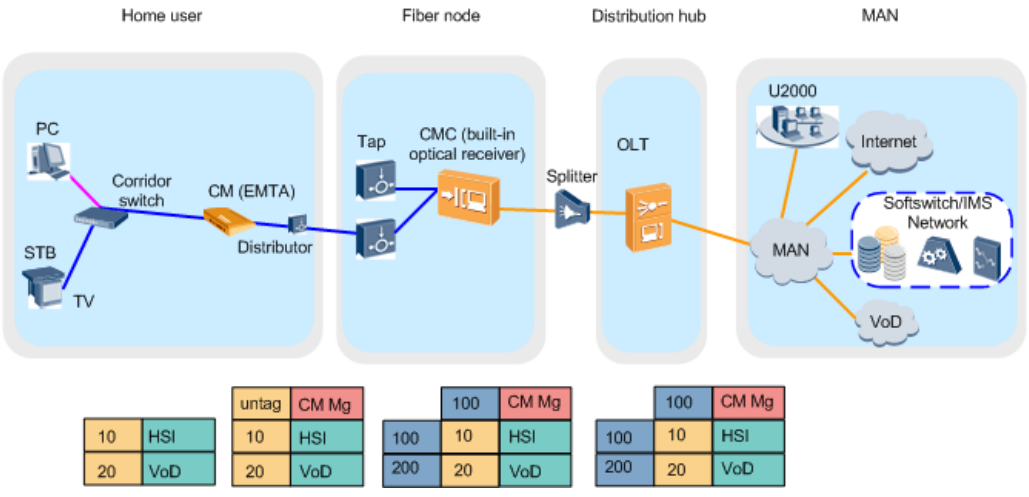
Figure 15-5 Multiple services in multiple VLANs (home access)



In the preceding network, IP addresses are allocated and service flows and VLAN tags are processed as follows:

1. The PC, STB, and CM use dynamic IP addresses allocated by a DHCP server.
2. All packets sent by the PC and STB are untagged.
3. The CMC adds VLAN tag 100 to the HSI service packets and CM management packets (CM Mg), adds VLAN tag 200 to the VoD service packets, and adds VLAN tag 300 to the VoIP service packets.

Figure 15-6 VLAN QinQ (home access)



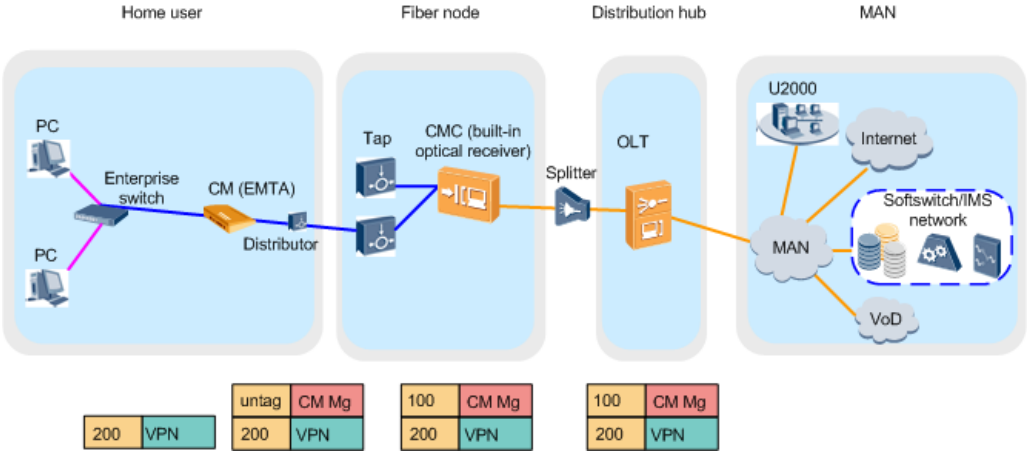
In the preceding network, IP addresses are allocated and service flows and VLAN tags are processed as follows:

1. The CM and STB use dynamic IP addresses allocated by a DHCP server. The PC uses PPPoE dialup.

Copyright © Huawei Technologies Co., Ltd.

2. All packets sent by the PC and STB are untagged. The corridor switch adds VLAN tag 10 to the HSI service packets and adds VLAN tag 20 to the VoD service packets.
3. The CMC adds VLAN tag 100 to the HSI service packets and CM management packets (CM Mg) and adds VLAN tag 200 to the VoD service packets.

Figure 15-7 VLAN tag transparent transmission (VPN access)



In the preceding network, IP addresses are allocated and service flows and VLAN tags are processed as follows:

1. The CM uses the dynamic IP address allocated by a DHCP server.
2. The enterprise switch statically configures the IP address of the PC and adds VLAN tag 200 to VPN data packets.
3. The CMC adds VLAN tag 100 to the CM management packets (CM Mg) and transparently transmits the VLAN tag of the VPN data packets.

NOTE

The preceding VLAN planning applies to the CMC, regardless of whether the CMC is deployed in standalone NE or centralized management mode.

Restrictions and Limitations

- In home access services, although the CMC supports multiple service VLANs (S-VLANs), all home access services are within the same broadcast domain. Therefore, the home access services do not support VLAN-based broadcast domains.
- In centralized management mode, one GPMD board supports a maximum of 1024 home access S-VLANs.

15.3 Service Configuration on a D-CMTS That Works as a GPON Remote Extended Frame on a Layer 3 Network

This section describes how to configure services, including home services, L2VPN enterprise service, and wireless local area network (WLAN) hotspot radio backhaul service, on an optical line terminal (OLT) when a distributed cable modem termination system (D-CMTS) works as a GPON extended frame on a Layer 3 network. The MA5603T equipped with the SCUV, GPMD, and SPUF boards is used as an example.

Copyright © Huawei Technologies Co., Ltd.

Control Board	SCUV
Cascading Board	GPMD: 0/3
SPU Board	SPUF: 0/4, 0/5

15.3.1 Home Service Networking

In home service networking, a distributed cable modem termination system (D-CMTS) connects to cable modems (CMs) at user homes through radio frequency (RF) ports and provides home services for users, including the cable TV (CATV) service, Internet access service, VoD service, broadband TV (BTV) service, and PacketCable service. This section describes how to configure the optical line terminal (OLT) to provision the home services.

NOTE

Configuration procedures are the same for IPv6 and IPv4 networks except in "Configure Dynamic Host Configuration Protocol (DHCP) relay" and "Configure a route". In addition, IPv6 does not support the function of configuring PacketCable dynamic voice services.

15.3.1.1 Service Requirements and Usage Scenario

Service Requirements

Users require the provisioning of the TV service, Internet access service, VoD service, broadband TV (BTV) service, and VoIP service. The TV service can be provisioned immediately after the distributed cable modem termination system (D-CMTS) hardware is connected. This section only describes how to configure the Internet access service, VoD service, BTV service, and VoIP service.

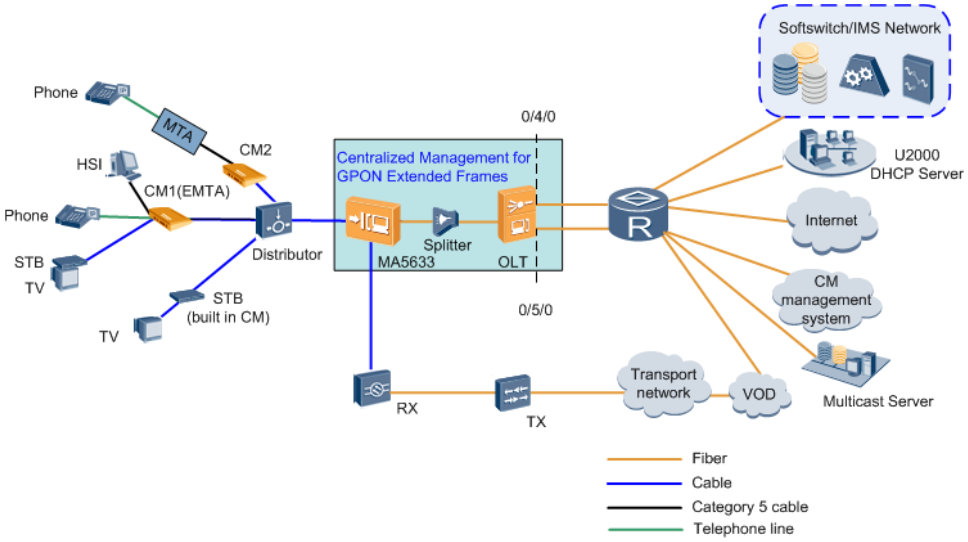
Usage Scenario

As shown in **Figure 15-8**, a D-CMTS is deployed on an optical node and cable modems (CMs) are deployed at user homes. The CMs connect to radio frequency (RF) ports on the MA5633 through cables.

- Port 1 on CM 1 connects to a PC for the Internet access service, port 2 connects to a phone set for the VoIP service, and the distributor connects to the STB for the VoD service. CM 1 supports embedded media terminal adapter (EMTA) functions and the voice users of CM 1 use PacketCable 1.x.
- CM 2 does not support EMTA functions and needs to connect to a media terminal adapter (MTA). The voice users of CM 2 use PacketCable Multimedia.
- Users access the Internet through Dynamic Host Configuration Protocol (DHCP) dialup.
- The IP addresses of the CM, STB, PC, and MTA are assigned by the DHCP server and in different network segments.
- The D-CMTS is used as a GPON remote extended frame. This reduces D-CMTS management and maintenance costs and simplifies configurations.

Copyright © Huawei Technologies Co., Ltd.

Figure 15-8 Home service networking

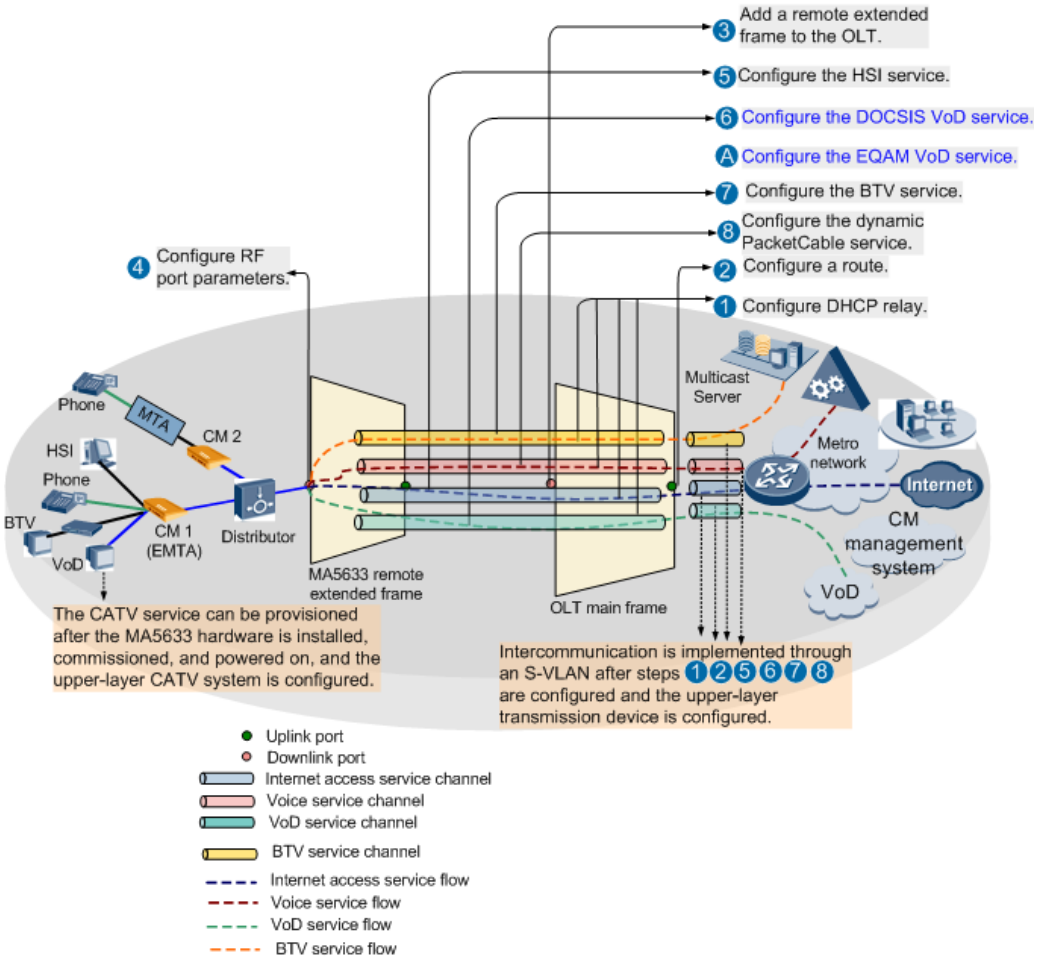


15.3.1.2 Configuration Process

Figure 15-9 shows the configuration roadmap for the home service networking.

Copyright © Huawei Technologies Co., Ltd.

Figure 15-9 Configuration roadmap for the home service networking



The following table describes configuration steps. All configurations are issued from the optical line terminal (OLT).

No.	Step	Description
1	● IPv4: **Configure Dynamic Host Configuration Protocol (DHCP) relay.** ● IPv6: **Configure Dynamic Host Configuration Protocol (DHCP) relay (IPv6).**	This section describes how to configure Dynamic Host Configuration Protocol (DHCP) relay so that cable modems (CMs) can obtain IP addresses in different network segments.
2	● IPv4: **Configure a route.** ● IPv6: **Configure a route (IPv6).**	This section describes how to implement network communication by configuring a route in Layer 3 networking with an optical line terminal (OLT). Through the route, packets are forwarded at Layer 3 between the OLT and its upper-layer devices or servers.

Copyright © Huawei Technologies Co., Ltd.

No.	Step	Description
3	**Add a remote extended frame to the OLT.**	An MA5633 that works as a remote extended frame connects to a port on a cascading board of an optical line terminal (OLT). You can configure the remote extended frame only after adding it to the OLT.
4	**Configure radio frequency (RF) port parameters.**	Radio frequency (RF) port parameters define the frequency spectrum range for signal transmission and modulation mode. The configuration of RF port parameters implements data service transmission over cables. RF port parameters can be configured using either of the following methods: ● Use a cable initialization profile to configure the parameters. ● Customize the parameters in cable mode.
5	**Configure the high-speed Internet (HSI) service.**	None
6	**Configure the DOCSIS VoD service.**	● If the MA5633 is not equipped with a built-in EQAM module, the MA5633 uses DOCSIS channels to transmit VoD data. ● If the MA5633 is equipped with a built-in EQAM module, the MA5633 sets idle downstream DOCSIS channels as EQAM channels to transmit VoD data. The DOCSIS VoD service and the EQAM VoD service are generally not concurrently used.
A	**Configure the EQAM VoD service.**	
7	**Configure the broadband TV (BTV) service.**	None
8	**Configure the dynamic PacketCable service.**	None

Copyright © Huawei Technologies Co., Ltd.

No.	Step	Description
9	**Verify the configured services.**	An OLT supports multiple remote service verification methods. This allows commissioning and configuration engineers to remotely verify services. 1. A DHCP dialup emulation test checks whether the OLT can communicate with the DHCP server and verifies CM DHCP configurations on the DHCP relay, proxy, and server. 2. The status of a CM can be queried. Based on the information, you can determine whether the CM is online.

15.3.1.3 Configuring DHCP Relay

This section describes how to configure Dynamic Host Configuration Protocol (DHCP) relay so that cable modems (CMs) can obtain IP addresses in different network segments.

Prerequisites

The upper-layer router, DHCP server, and Trivial File Transfer Protocol (TFTP) server of an optical line terminal (OLT) have been configured.

Data Plan

Table 15-5 DHCP data plan for the OLT

Item	Data
VLAN	ID of the CM management S-VLAN: 100; type of the VLAN: smart
DHCP server group parameters	● IP address of the DHCP domain gateway for CMs: 10.10.224.1; domain name: docsis ● IP address of the DHCP domain gateway for media terminal adapters (MTAs): 10.100.224.1; domain name: pktc ● IP address of the DHCP domain gateway for paid PCs: 10.100.187.1; domain name: default ● IP address of the DHCP domain gateway for overdue PCs: 10.100.8.1; domain name: default ● IP address of the DHCP domain gateway for set top boxes (STB): 10.200.160.1; domain name: stb

Copyright © Huawei Technologies Co., Ltd.

Table 15-6 Data plan for the upper-layer devices of the OLT

Item	IP Address
Layer 3 interfaces connecting the router to the OLT	● Forwarding DHCP and broadband packets: 11.11.11.11 ● Forwarding CM management, VoD, and multicast packets: 11.11.12.11
IP addresses of DHCP servers	● DHCP server assigning IP addresses to CMs and MTAs: 192.168.10.10-192.168.10.11 ● DHCP server assigning IP addresses to PCs and STBs: 192.168.10.12-192.168.10.13
IP address of the TFTP server	192.168.5.10-192.168.5.13

Procedure

Step 1 Set the IP addresses of Layer 3 VLAN interfaces.

```
huawei(config)#vlan 100 smart
huawei(config)#interface vlanif 100
huawei(config-if-vlanif100)#arp proxy enable
huawei(config-if-vlanif100)#ip address 10.10.224.1 255.255.255.0 description
docsis     //Set the IP address of the DHCP domain gateway for CMs.
huawei(config-if-vlanif100)#ip address 10.100.224.1 255.255.255.0 sub description
pktc     //Set the IP address of the DHCP domain gateway for MTAs.
huawei(config-if-vlanif100)#ip address 10.200.160.1 255.255.255.0 sub description
stb     //Set the IP address of the DHCP domain gateway for STBs.
huawei(config-if-vlanif100)#ip address 10.100.187.1 255.255.255.0 sub description
default     //Set the IP address of the DHCP domain gateway for paid PCs.
huawei(config-if-vlanif100)#ip address 10.100.8.1 255.255.255.0 sub description
default      //Set the IP address of the DHCP domain gateway for overdue PCs.
huawei(config-if-vlanif100)#quit
```

Step 2 Configure the working mode of the DHCP relay to Layer 3 Option 60.

In DHCP Option 60 mode, a DHCP server group is selected according to the Option 60 domain name in DHCP packets. Users in this mode are identified by domain information of packets, which differentiates various service types in a VLAN. Ensure that the Option 60 domain name and the DHCP server group bound to the Option 60 domain name are configured beforehand.

```
huawei(config)#dhcp mode layer-3 Option60
  Several minutes may be required and no action can be taken during this period
  Are you sure to perform this operation? (y/n)[n]: y
```

Step 3 Enable the DHCP option82 feature.

The DHCP feature does not have any mechanism for authentication or security. Thus, the DHCP feature encounters many security problems when it is used in the network. To solve these problems, the DHCP option82 is introduced.

```
huawei(config)#dhcp option82 enable
```

Step 4 Set the IP addresses of the servers in a DHCP server group.

```
huawei(config)#dhcp-server 0 ip 192.168.10.10 192.168.10.11    //Configure DHCP
server group 0 to assign IP addresses to CMs and MTAs.
```


Copyright © Huawei Technologies Co., Ltd.

```
huawei(config)#dhcp-server 1 ip 192.168.10.12 192.168.10.13    //Configure DHCP
server group 1 to assign IP addresses to PCs and STBs.
```

Step 5 Create a DHCP Option 60 domain.

```
huawei(config)#dhcp domain default   //Create Option 60 domain name default for
PCs.
huawei(config-dhcp-domain-default)#dhcp-gateway learning enable   //Paid and
overdue PCs are in different network segments. Therefore, self-learning needs to be
enabled on OLT gateways.
huawei(config-dhcp-domain-default)#dhcp-server 1 vlan 100       //Bind DHCP server
group 1 to the DHCP domain where the PCs locate. After the configuration, the PCs
in the DHCP domain are corresponded to DHCP server group 1.
huawei(config-dhcp-domain-default)#quit
huawei(config)#dhcp domain docsis   //Create Option 60 domain name docsis for CMs.
huawei(config-dhcp-domain-docsis)#dhcp-server 0 vlan 100       //Bind DHCP server
group 0 to the DHCP domain where the CMs locate. After the configuration, the CMs
in the DHCP domain are corresponded to DHCP server group 0.
huawei(config-dhcp-domain-docsis)#quit
huawei(config)#dhcp domain pktc   //Create Option 60 domain name pktc for MTAs.
huawei(config-dhcp-domain-pktc)#dhcp-server 0 vlan 100       //Bind DHCP server
group 0 to the DHCP domain where the MTAs locate. After the configuration, the CMs
in the DHCP domain are corresponded to DHCP server group 0.
huawei(config-dhcp-domain-pktc)#quit
huawei(config)#dhcp domain stb   //Create Option 60 domain name stb for STBs.
huawei(config-dhcp-domain-stb)#dhcp-server 1 vlan 100     //Bind DHCP server group
1 to the DHCP domain where the STBs locate. After the configuration, the STBs in
the DHCP domain are corresponded to DHCP server group 1.
huawei(config-dhcp-domain-stb)#quit
```

Step 6 Set IP addresses of the gateways for the DHCP domain.

```
huawei(config)#interface vlanif 100
huawei(config-if-vlanif100)#dhcp domain default gateway 10.100.187.1
10.100.8.1    //Set the IP address of the gateway for the PC domain to 10.100.187.1
for paid PCs and to 10.100.8.1 for overdue PCs.
huawei(config-if-vlanif100)#dhcp domain docsis gateway 10.10.224.1    //Set the IP
address of the gateway for the CM domain to 10.10.224.1.
huawei(config-if-vlanif100)#dhcp domain pktc gateway 10.100.224.1    //Set the IP
address of the gateway for the MTA domain to 10.100.224.1.
huawei(config-if-vlanif100)#dhcp domain stb gateway 10.200.160.1    //Set the IP
address of the gateway for the STB domain to 10.200.160.1.
huawei(config-if-vlanif100)#quit
```

----End

15.3.1.4 Configuring a Route

This section describes how to implement network communication by configuring a route in Layer 3 networking with an optical line terminal (OLT). Through the route, packets are forwarded at Layer 3 between the OLT and its upper-layer devices or servers.

Prerequisites

The upper-layer router has been configured.

Copyright © Huawei Technologies Co., Ltd.

Data Plan

Table 15-7 Data plan for the Layer 3 interfaces on the network side

Item	IP Address
Layer 3 interfaces on the OLT network side	Forwarding Dynamic Host Configuration Protocol (DHCP) and broadband packets: ● VLAN ID: 2004 ● Port number: 0/4/0 ● IP address: 11.11.11.10/24 Forwarding cable modem (CM) management, VoD, and multicast packets: ● VLAN ID: 2005 ● Port number: 0/5/0 ● IP address: 11.11.12.10/24
Layer 3 interfaces connecting the router to the OLT	● Forwarding DHCP and broadband packets: 11.11.11.11 ● Forwarding CM management, VoD, and multicast packets: 11.11.12.11
Upper-layer servers of the OLT	● DHCP servers: – DHCP server assigning IP addresses to CMs and media terminal adapters (MTAs): 192.168.10.10-192.168.10.11 – DHCP server assigning IP addresses to PCs and set top boxes (STBs): 192.168.10.12-192.168.10.13 ● CM management system, VoD server, and multicast server: 192.168.20.10-192.168.20.12 ● Softswitch or IP multimedia subsystem (IMS) server: 192.168.50.10

Procedure

Step 1 Create Layer 3 VLAN interfaces on the network side.

1. Create VLANs and configure their uplink ports.
   - VLAN 2004 is of the smart VLAN type and used for forwarding DHCP and broadband packets. Add uplink port 0/4/0 to VLAN 2004.
   - VLAN 2005 is of the smart VLAN type and used for forwarding CM management, VoD, and multicast packets. Add uplink port 0/5/0 to VLAN 2005.

```
huawei(config)#vlan 2004 to 2005 smart
huawei(config)#port vlan 2004 0/4 0
huawei(config)#port vlan 2005 0/5 0
```

2. (Optional) Create native VLANs for Ethernet outbound ports.

   Packets between the OLT and its upper-layer router are assumed to be forwarded at Layer 3 and no VLAN information is required. The created native VLANs remove VLAN tags from the packets transmitted out of Ethernet ports.

Copyright © Huawei Technologies Co., Ltd.

```
huawei(config)#interface eth 0/4
huawei(config-if-eth-0/4)#native-vlan 0 vlan 2004    //Remove VLAN tags from
the packets transmitted out of the 0/8/0 port.
huawei(config-if-eth-0/4)#quit
huawei(config)#interface eth 0/5
huawei(config-if-eth-0/5)#native-vlan 0 vlan 2005    //Remove VLAN tags from
the packets transmitted out of the 0/9/0 port.
huawei(config-if-eth-0/5)#quit
```

3. Create Layer 3 VLAN interfaces.

   a. Create a Layer 3 interface for VLAN 2004, through which DHCP and broadband packets are forwarded.

   ```
   huawei(config)#interface vlanif 2004
   huawei(config-if-vlanif2004)#ip address 11.11.11.10 255.255.255.0
   huawei(config-if-vlanif2004)#quit
   ```

   b. Create a Layer 3 interface for VLAN 2005, through which CM management and VoD packets are forwarded.

   ```
   huawei(config)#interface vlanif 2005
   huawei(config-if-vlanif2005)#ip address 11.11.12.10 255.255.255.0
   huawei(config-if-vlanif2005)#quit
   ```

Step 2 Configure static routes to implement the communication between the OLT and its upper-layer devices.

```
huawei(config)#ip route-static 0.0.0.0 0.0.0.0 11.11.11.11     //Broadband packets
are forwarded through the Layer 3 interface of VLAN 2004.
huawei(config)#ip route-static 192.168.20.0 255.255.255.0 11.11.12.11     //CM
management, VoD, and multicast packets are forwarded through the Layer 3 interface
of VLAN 2005.
huawei(config)#ip route-static 192.168.60.3 255.255.255.0 11.11.12.11     //COPS
packets are forwarded through the Layer 3 interface of VLAN 2005.
huawei(config)#ip route-static 192.168.10.0 255.255.255.0 11.11.11.11     //DHCP
packets are forwarded through the Layer 3 interface of VLAN 2004.
huawei(config)#ip route-static 192.168.5.0 255.255.255.0 11.11.12.11      //TFTP
server
huawei(config)#ip route-static 192.168.50.0 255.255.255.0 11.11.12.11     //
Softswitch or IMS server
```

NOTE

The interconnected router must set static routes and add the routes to dynamic routes.

----End

Result

The OLT can communicate with its upper-layer devices. To check network connectivity between two devices, run the **ping** and **tracert** commands.

The configured static routes can be queried in an IPv4 routing table by running the **display ip routing-table** command.

15.3.1.5 Configuring DHCP Relay (IPv6)

This section describes how to configure DHCPv6 relay so that terminals can obtain IP addresses in different network segments.

Prerequisites

The upper-layer router and DHCP server have been configured.

Copyright © Huawei Technologies Co., Ltd.

Data Plan

Table 15-8 DHCP data plan

Configuration Item	Data
Terminal-side of CM	● network segment of CM: 2001:0db8:0001::/64 ● network segment of PCs with fees paid: 2001:0db8:0003::/64 ● network segment of overdue PCs: 2001:0db8:0004::/64
User-side of OLT	● IP address of the gateway for the DHCP domain of CMs: 2001:0db8:0001::1/64; domain name: **docsis** ● IP address of the gateway for the DHCP domain of PCs with fees paid: 2001:0db8:0003::3/64; domain name: **default** ● IP address of the gateway for the DHCP domain of overdue PCs: 2001:0db8:0004::4/64; domain name: **default**
Network-side of OLT	Forwarding DHCP and broadband packets: ● VLAN ID: 2004 ● Port number: 0/4/0 ● IP address: 2001:0db8:0007::12/64 Forwarding CM management packets, multicast packets, and VoD packets: ● VLAN ID: 2005 ● Port number: 0/5/0 ● IP address: 2001:0db8:0008::13/64
Router	● IP address of the Layer 3 interface for forwarding DHCP and broadband packets: 2001:0db8:0007::6/64 ● IP address of the Layer 3 interface for forwarding CM management packets: 2001:0db8:0008::7/64
Server	● IP addresses of DHCP servers: – DHCP server allocating IP addresses for CMs: 2001:0db8:0006::8/64-2001:0db8:0006::9/64 – DHCP server allocating IP addresses for PCs: 2001:0db8:0006::10/64-2001:0db8:0006::11/64 ● IP addresses of the CM management system: 2001:0db8:0011::14/64-2001:0db8:0011::16/64

Procedure

Step 1 Configure a CM service provisioning mode, which can be IPv6 (preferentially used), APM, or DPM (used for dual-stack service provisioning). Select a mode based on site requirements.

Copyright © Huawei Technologies Co., Ltd.

```
huawei(config)#interface cable 1/1/0
huawei(config-if-cable-1/1/0)#cable ip-mode dpm
huawei(config-if-cable-1/1/0)#quit
```

Step 2 Configure the IP address of the VLAN Layer 3 interface.

```
huawei(config)#ipv6      //Enable IPv6 packet forwarding.
huawei(config)#vlan 100
huawei(config)#interface vlanif 100
huawei(config-if-vlanif100)#ipv6 enable     //Enable IPv6 on ports.
huawei(config-if-vlanif100)#undo ipv6 nd ra halt       //enables a router to send
RA messages.
huawei(config-if-vlanif100)#ipv6 nd autoconfig managed-address-flag    //Configure
the state-based auto-configuration address flag bit. The host obtains an IPv6
address using the state-based automatic configuration.
huawei(config-if-vlanif100)#ipv6 address 2001:0db8:0001::1/64     //Configure the
IP address of the gateway for the DHCP domain of CMs.
huawei(config-if-vlanif100)#ipv6 address 2001:0db8:0003::3/64     //Configure the
IP address of the gateway for the DHCP domain of PCs with fees paid.
huawei(config-if-vlanif100)#ipv6 address 2001:0db8:0004::4/64     //Configure the
IP address of the gateway for the DHCP domain of overdue PCs.
huawei(config-if-vlanif100)#quit
```

Step 3 Enable duplicate address detect (DAD) proxy, which prevents repeated link local addresses (LLAs) on the user side.

After receiving a DAD packet sent from the user side with destination IP address LLA, the OLT with DAD proxy enabled checks user online information based on the destination IP address and VLAN. If a user with the same IP address in the VLAN has been online, the OLT makes a response and prohibits the new user from going online. Otherwise, the OLT does not make a response.

```
huawei(config)#ipv6 dad proxy enable
huawei(config)#vlan service-profile profile-id 10
huawei(config)#vlan bind service-profile 100 profile-id 10
huawei(config-vlan-srvprof-10)#ipv6 dad proxy enable     //DAD proxy takes effect
after it is enabled at system level and VLAN service profile level.
```

Step 4 Configure the working mode of DHCP relay to Layer 3 Option 16.

Option 16 is an option with code 16 in DHCPv6 packets, which identifies terminal types. In DHCPv6 Option 16 mode, packets select a DHCPv6 server based on the Option 16 domain. Therefore, in DHCPv6 Option 16 mode, packets select a DHCPv6 server based on terminal types.

```
huawei(config)#dhcpv6 mode layer-3 option16
  Several minutes may be required and no action can be taken during this period
  Are you sure to perform this operation? (y/n)[n]: y
```

Step 5 Enable DHCPv6 Option.

No authentication and security mechanisms are available for DHCPv6. Therefore, the application of DHCPv6 faces multiple security issues on networks. The enabled DHCPv6 Option function resolves these issues.

```
huawei(config)#dhcpv6 option enable
```

Step 6 Configure the IP addresses of the servers in a DHCP server group.

```
huawei(config)#dhcpv6-server 0 ipv6 2001:0db8:0006::8/64 2001:0db8:0006::9/64    //
Configure DHCP server group 0 to allocate IP addresses for CMs.
huawei(config)#dhcpv6-server 1 ipv6 2001:0db8:0006::10/64
2001:0db8:0006::11/64    //Configure DHCP server group 1 to allocate IP addresses
for PCs.
```

Step 7 Create DHCP Option 16 domains.

Copyright © Huawei Technologies Co., Ltd.

```
huawei(config)#dhcp domain default   //Create Option 16 domain default for PCs.
huawei(config-dhcp-domain-default)#dhcpv6-gateway learning enable   //PCs require
different IP address segments based on fee payment state. Therefore, automatic
gateway learning must be enabled on the OLT.
huawei(config-dhcp-domain-default)#dhcpv6-server 1 vlan 100        /Bind DHCP
server group 1 to the DHCP domain of PCs. After the configuration, the PCs in this
DHCP domain are mapped to DHCP server group 1.
huawei(config-dhcp-domain-default)#quit
huawei(config)#dhcp domain docsis   //Create Option 16 domain docsis for CMs.
huawei(config-dhcp-domain-docsis)#dhcpv6-server 0 vlan 100      //Bind DHCP server
group 0 to the DHCP domain of CMs. After the configuration, the CMs in this DHCP
domain are mapped to DHCP server group 0.
huawei(config-dhcp-domain-docsis)#quit
```

Step 8 Configure the IP addresses of the gateways for DHCP domains.

```
huawei(config)#interface vlanif 100
huawei(config-if-vlanif100)#dhcp domain default gateway ipv6 2001:0db8:0003::3/64
2001:0db8:0004::4/64    //Configure IP addresses of the gateways for the DHCP
domain of PCs, including the IP address of the gateway for the PCs with fees paid
and the IP address of the gateway for overdue PCs.
huawei(config-if-vlanif100)#dhcp domain docsis gateway ipv6
2001:0db8:0001::1/64    //Configure the IP address of the gateway for the DHCP
domain of CMs.

huawei(config-if-vlanif100)#quit
```

----End

15.3.1.6 Configuring a Route (IPv6)

This section describes how to implement network communication by configuring a route in Layer 3 networking with an OLT. Through the route, the OLT can forward packets at Layer 3 between the OLT and its upper-layer devices or servers.

Prerequisites

The upper-layer router of the OLT has been configured.

Data Plan

Table 15-9 DHCP data plan

Configuration Item	Data
Terminal-side of CM	● network segment of CM: 2001:0db8:0001::/64 ● network segment of PCs with fees paid: 2001:0db8:0003::/64 ● network segment of overdue PCs: 2001:0db8:0004::/64
User-side of OLT	● IP address of the gateway for the DHCP domain of CMs: 2001:0db8:0001::1/64; domain name: **docsis** ● IP address of the gateway for the DHCP domain of PCs with fees paid: 2001:0db8:0003::3/64; domain name: **default** ● IP address of the gateway for the DHCP domain of overdue PCs: 2001:0db8:0004::4/64; domain name: **default**

Copyright © Huawei Technologies Co., Ltd.

Configuration Item	Data
Network-side of OLT	Forwarding DHCP and broadband packets: ● VLAN ID: 2004 ● Port number: 0/4/0 ● IP address: 2001:0db8:0007::12/64 Forwarding CM management packets, multicast packets, and VoD packets: ● VLAN ID: 2005 ● Port number: 0/5/0 ● IP address: 2001:0db8:0008::13/64
Router	● IP address of the Layer 3 interface for forwarding DHCP and broadband packets: 2001:0db8:0007::6/64 ● IP address of the Layer 3 interface for forwarding CM management packets: 2001:0db8:0008::7/64
Server	● IP addresses of DHCP servers: – DHCP server allocating IP addresses for CMs: 2001:0db8:0006::8/64-2001:0db8:0006::9/64 – DHCP server allocating IP addresses for PCs: 2001:0db8:0006::10/64-2001:0db8:0006::11/64 ● IP addresses of the CM management system: 2001:0db8:0011::14/64-2001:0db8:0011::16/64

Procedure

Step 1 Create VLAN Layer 3 interfaces on the network side.

1. Create VLANs and add an uplink port to them, respectively.
   - VLAN 2004 used for forwarding DHCP and broadband packets is a smart VLAN. Add uplink port 0/4/0 to VLAN 2004.
   - VLAN 2005 used for forwarding CM management packets, multicast packets, and VoD packets is a smart VLAN. Add uplink port 0/5/0 to VLAN 2005.

```
huawei(config)#vlan 2004 to 2005 smart
huawei(config)#port vlan 2004 0/4 0
huawei(config)#port vlan 2005 0/5 0
```

2. (Optional) Create native VLANs for Ethernet outbound ports.

   Packets between the OLT and its upper-layer router are forwarded at Layer 3 and no VLAN tag is required. The created native VLANs remove VLAN tags from the packets transmitted out of Ethernet ports.

```
huawei(config)#interface eth 0/4
huawei(config-if-eth-0/4)#native-vlan 0 vlan 2004    //The packets transmitted
out of port 0/4/0 are untagged.
huawei(config-if-eth-0/4)#quit
huawei(config)#interface eth 0/5
huawei(config-if-eth-0/5)#native-vlan 0 vlan 2005    //The packets transmitted
```


Copyright © Huawei Technologies Co., Ltd.

```
out of port 0/5/0 are untagged.
huawei(config-if-eth-0/5)#quit
```

3. Create VLAN Layer 3 interfaces.

   a. Create the Layer 3 interface of VLAN 2004, through which DHCP and broadband packets are forwarded.

   ```
   huawei(config)#interface vlanif 2004
   huawei(config-if-vlanif2004)#ipv6 address 2001:0db8:0007::12/64
   huawei(config-if-vlanif2004)#quit
   ```

   b. Create the Layer 3 interface of VLAN 2005, through which CM management packets, multicast packets, and VoD packets are forwarded.

   ```
   huawei(config)#interface vlanif 2005
   huawei(config-if-vlanif2005)#ipv6 address 2001:0db8:0008::13/64
   huawei(config-if-vlanif2005)#quit
   ```

Step 2 Configure static routes for the communication between the OLT and its upper-layer devices.

```
huawei(config)#ipv6 route-static ::/0 2001:0db8:0007::6/64     //Broadband packets
are forwarded through the Layer 3 interface of VLAN 2004.
huawei(config)#ipv6 route-static 2001:0db8:0011::/64 2001:0db8:0008::7/64     //CM
management packets are forwarded through the Layer 3 interface of VLAN 2005.
huawei(config)#ipv6 route-static 2001:0db8:0006::/64 2001:0db8:0007::6/64     //
DHCP packets are forwarded through the Layer 3 interface of VLAN 2004.
```

NOTE

Configure static routes on the router connected to the OLT. In addition, add the static routes to dynamic ones.

----End

Result

The OLT can communicate with its upper-layer devices. To check network connectivity between two devices, run the **ping ipv6** and **tracert ipv6** commands.

The configured static routes can be queried in an IPv6 routing table by running the **display ipv6 routing-table** command.

15.3.1.7 Adding a Remote Extended Frame to an OLT

An MA5633 that works as a remote extended frame connects to a port on a cascading board of an optical line terminal (OLT). You can configure the remote extended frame only after adding it to the OLT.

Prerequisites

The MA5633 management policy is set to **extend-frame**. To do so, run the **sysman centralized-mgmt primary** command.

Context

A GPON remote extended frame is added to an OLT in the following two steps: Add the MA5633 to the OLT as a GPON optical network unit (ONU). Then add the MA5633 to the OLT as a GPON remote extended frame.

You can use either of the methods listed in the following table to add a remote extended frame to an OLT based on site requirements.

Copyright © Huawei Technologies Co., Ltd.

Table 15-10 Methods of adding a remote extended frame to an OLT

Method	Usage Scenario	Remarks
Add a remote extended frame in offline mode.	A carrier has planned all remote extended frame IDs together and the remote extended frames must be deployed one by one. This method facilitates remote extended frame management.	1. You have obtained the serial number (SN) of the remote extended frame. 2. The remote extended frame ID has been planned.
Add an automatically discovered remote extended frame.	A great number of remote extended frames need to be deployed. This method reduces manual configurations.	1. You do not know the SN of the remote extended frame. 2. The remote extended frame ID does not need to be planned.

Data Plan

Table 15-11 Data plan

Item	Data
GPON cascading board	Board: H801GPMD Port ID: 0/3/1 Remote extended frame ID: 1 Remote extended frame authentication mode: SN Remote extended frame SN: 48575443E6D8B541 **NOTE** The OLT uses the MA5603T as an example. The configuration method is the same for other OLTs. The only difference lies in slot IDs.
Dynamic bandwidth allocation (DBA)	Profile: default Type: type4 Maximum bandwidth: 1000 Mbit/s
Line profile	Profile: default GPON encapsulation mode (GEM) port ID: 0 (fixed port in centralized management mode) Transmission container (T-CONT) ID: 1 (fixed T-CONT in centralized management mode)
MA5633 management mode	extend-frame

Copyright © Huawei Technologies Co., Ltd.

Procedure

- Add a remote extended frame in offline mode.

  ```
  huawei(config)#frame add 1 MA5633 extending-port 0/3/1 sn 48575443E6D8B541
  ```

  NOTE

  When running the **frame add** command to add a remote extended frame in offline mode, the OLT automatically allocates a temporary SN for the remote extended frame. Therefore, you do not need to specify the SN of the remote extended frame. After obtaining the SN of the remote extended frame, run the **frame bind** command to add the binding relationship between the SN and the remote extended frame to the OLT. Then the remote extended frame is added.

- Add an automatically discovered remote extended frame.

  The OLT supports the adding of an automatically discovered GPON remote extended frame. This function does not require manual confirmation, thereby simplifying the remote extended frame registration and adding flow.

  ```
  huawei(config)#interface gpon 0/3
  huawei(config-if-gpon-0/3)#port 1 ont-auto-find enable
  huawei(config-if-gpon-0/3)#quit
  ```

----End

Result

The remote extended frame is online.

After adding the remote extended frame, run the **display frame info** command to query the status of the remote extended frame. Ensure that **Online state** is **online** and **State** is **normal**.

```
huawei(config)#display frame info 1
  ---------------------------------------------------------------------------
  Type:           MA5633
  State:          Normal
  Desc:           MA5633_1_extending_0/3/1/1
  Hardware:       MA5633
  Extend type:    GPON
  Extending port: 0 /3 /1
  ONT ID:         1
  ONT SN:         48575443E6D8B541
  Extended port:  1 /0 /1
  Online state:   Online
  Optical-receiver: Offline
  ---------------------------------------------------------------------------
```

Follow-up Procedure

If the remote extended frame cannot be discovered, follow the troubleshooting suggestions listed in the following table to rectify faults.

Possible Cause	Troubleshooting Suggestion
The MA5633 automatic discovery function is disabled.	In GPON mode, run the **port ont-auto-find** command to enable the MA5633 automatic discovery function on GPON ports.

Copyright © Huawei Technologies Co., Ltd.

Possible Cause	Troubleshooting Suggestion
The MA5633 works as a standalone NE and cannot work as a remote extended frame.	Replace the MA5633 with the one that works as a remote extended frame.
The MA5633 management policy is set to **stand-alone** on the OLT.	Run the **sysman centralized-mgmt primary** command to configure the MA5633 management policy to **extend-frame**.
The number of remote extended frames on the OLT has reached the threshold.	Run the **frame delete** command to delete a remote extended frame that is no longer used from the OLT.

15.3.1.8 Configuring RF Port Parameters

Radio frequency (RF) port parameters define the frequency spectrum range for signal transmission and modulation mode. The configuration of RF port parameters implements data service transmission over cables.

Context

You can use either of the methods listed in the following table to configure RF port parameters based on site requirements.

Copyright © Huawei Technologies Co., Ltd.

Table 15-12 Methods of configuring RF port parameters

Method	Usage Scenario	Remarks
Use a cable initialization profile to configure RF port parameters.	A carrier needs to deploy remote extended frames in batches. This method reduces data configuration for remote extended frames, thereby improving service provisioning efficiency. Configure the RF parameter profile for the remote extended frames on the optical line terminal (OLT). After the remote extended frames are powered on and added to the OLT, the OLT automatically issues the RF parameter profile to the remote extended frames, without requiring any software configuration. **NOTE** After the cable initialization profile is configured, a remote extended frame uses the RF port parameters configured in the profile after going online, regardless of whether the remote extended frame in added in offline mode or automatically discovered by the OLT.	● If the RF port parameters are the same for all the remote extended frames to be deployed in batches, use the cable initialization profile to configure the parameters. ● If the RF port parameters are basically the same for all the remote extended frames to be deployed in batches, use the cable initialization profile to configure the parameters. Then modify parameter settings in customized cable configuration mode.
Customize RF port parameters in cable mode.	Requires differentiated plans and configurations for RF port parameters of remote extended frames and the remote extended frames must be configured one by one.	If the RF port parameters are greatly different for the remote extended frames to be deployed in batches, use this method to configure the parameters.

Data Plan

Table 15-13 Data plan for RF port parameters

Item	Data
RF port	1/1/0

Copyright © Huawei Technologies Co., Ltd.

Item	Data
Upstream channels	● IDs: 1-4 ● Type: European standard (default channel type) ● ID of the upstream channel modulation profile: 1 (by default) ● Channel central frequency (MHz): 29.8, 42.60, 49.00, and 55.4
Downstream channels	● IDs: 1-16 ● Type: European standard (default channel type) ● Channel central frequency (MHz): 602.00, 610.00, 618.00, ..., and 722.00

Procedure

- Use a cable initialization profile to configure RF port parameters.
  1. Configure the frequency spectrum range and channel type.

     In this example, the channel is of the European type. To change the type to North American, run the **cable** command.
  2. Configure RF port parameters for upstream channels and activate the upstream channels.

Parameter	Description
frequency and **channel-width**	A central frequency and a frequency bandwidth determine a frequency range, within which packets are transmitted. For example, the central frequency of a European channel is 55 MHz and the frequency bandwidth is 6400 kHz. Then the frequency range of the channel is 51.8-58.2 MHz.
modulation-profile	An upstream channel modulation profile defines parameters for processing the signals transmitted over the upstream channel. You do not need to configure an upstream channel modulation profile generally. Ports automatically bind to profile 1 by default.

The following configurations are used as an example to configure RF parameters for upstream channels:

- Number of upstream channels: 4
- Frequency bandwidth of the channels: 3.2 MHz (default value)

```
huawei(config)#interface cable init-template
huawei(config-cable-init-template)#cable upstream 1 frequency 29.8 enable
huawei(config-cable-init-template)#cable upstream 2 frequency 42.60
```


Copyright © Huawei Technologies Co., Ltd.

```
enable
huawei(config-cable-init-template)#cable upstream 3 frequency 49.00
enable
huawei(config-cable-init-template)#cable upstream 4 frequency 55.40
enable
```

3. Configure RF port parameters for downstream channels and activate the downstream channels.

Parameter	Description
modulation	A greater modulation mode value for downstream channels results in a higher channel bandwidth but weaker anti-interference capability. Therefore, configure the modulation mode based on site requirements. The default modulation mode is QAM256. This example uses the default setting.

The following configuration is used as an example to configure RF parameters for downstream channels: A total of 16 downstream channels have been purchased.

```
huawei(config-cable-init-template)#cable downstream 1 frequency 602.00
enable
huawei(config-cable-init-template)#cable downstream 2 frequency 610.00
enable
huawei(config-cable-init-template)#cable downstream 3 frequency 618.00
enable
huawei(config-cable-init-template)#cable downstream 4 frequency 626.00
enable
huawei(config-cable-init-template)#cable downstream 5 frequency 634.00
enable
huawei(config-cable-init-template)#cable downstream 6 frequency 642.00
enable
huawei(config-cable-init-template)#cable downstream 7 frequency 650.00
enable
huawei(config-cable-init-template)#cable downstream 8 frequency 658.00
enable
huawei(config-cable-init-template)#cable downstream 9 frequency 666.00
enable
huawei(config-cable-init-template)#cable downstream 10 frequency 674.00
enable
huawei(config-cable-init-template)#cable downstream 11 frequency 682.00
enable
huawei(config-cable-init-template)#cable downstream 12 frequency 690.00
enable
huawei(config-cable-init-template)#cable downstream 13 frequency 698.00
enable
huawei(config-cable-init-template)#cable downstream 14 frequency 706.00
enable
huawei(config-cable-init-template)#cable downstream 15 frequency 714.00
enable
huawei(config-cable-init-template)#cable downstream 16 frequency 722.00
enable
```

- Customize the RF port parameters in cable mode.

  NOTE

  The configuration is complete if you have configured the RF port parameters using a cable initialization profile. For details, see **Use a cable initialization profile to configure RF port parameters**. Perform this operation if you need to customize the RF port parameters of a remote extended frame.

Copyright © Huawei Technologies Co., Ltd.

1. Configure RF port parameters for upstream channels and activate the upstream channels.

```
huawei(config)#interface cable 1/1/0
huawei(config-if-cable-1/1/0)#cable upstream 1 frequency 29.8 enable
huawei(config-if-cable-1/1/0)#cable upstream 2 frequency 42.60 enable
huawei(config-if-cable-1/1/0)#cable upstream 3 frequency 49.00 enable
huawei(config-if-cable-1/1/0)#cable upstream 4 frequency 55.40 enable
```

2. Configure RF port parameters for downstream channels and activate the downstream channels.

```
huawei(config-if-cable-1/1/0)#cable downstream 1 frequency 602.00 enable
huawei(config-if-cable-1/1/0)#cable downstream 2 frequency 610.00 enable
huawei(config-if-cable-1/1/0)#cable downstream 3 frequency 618.00 enable
huawei(config-if-cable-1/1/0)#cable downstream 4 frequency 626.00 enable
huawei(config-if-cable-1/1/0)#cable downstream 5 frequency 634.00 enable
huawei(config-if-cable-1/1/0)#cable downstream 6 frequency 642.00 enable
huawei(config-if-cable-1/1/0)#cable downstream 7 frequency 650.00 enable
huawei(config-if-cable-1/1/0)#cable downstream 8 frequency 658.00 enable
huawei(config-if-cable-1/1/0)#cable downstream 9 frequency 666.00 enable
huawei(config-if-cable-1/1/0)#cable downstream 10 frequency 674.00 enable
huawei(config-if-cable-1/1/0)#cable downstream 11 frequency 682.00 enable
huawei(config-if-cable-1/1/0)#cable downstream 12 frequency 690.00 enable
huawei(config-if-cable-1/1/0)#cable downstream 13 frequency 698.00 enable
huawei(config-if-cable-1/1/0)#cable downstream 14 frequency 706.00 enable
huawei(config-if-cable-1/1/0)#cable downstream 15 frequency 714.00 enable
huawei(config-if-cable-1/1/0)#cable downstream 16 frequency 722.00 enable
```

----End

Result

1. The transmit power of the downstream channels meets site requirements.

   Run the **display cable downstream** *frameid/slotid/portid* { **all** | *channel-id* } **status** command to check whether the RF port parameters meet site requirements.

2. The signal-to-noise (SNR) ratio of the upstream channels meets site requirements.

   Run the **display cable signal quality** [*frameid/slotid/portid* [**upstream** *channel-id*]] command to check whether the RF port parameters meet site requirements. A greater SNR ratio results in better signal quality. The recommended SNR ratio is greater than 30 dB.

15.3.1.9 Configuring the HSI Service

A cable modem (CM) connects to a distributed cable modem termination system (D-CMTS) through a cable and provides the high-speed Internet (HSI) service for users.

Data Plan

Table 15-14 Data plan for the HSI service

Item	Data
VLAN	ID of the HSI service VLAN (S-VLAN): 100; type of the VLAN: smart

Copyright © Huawei Technologies Co., Ltd.

Item	Data
Uplink ports	Forwarding Dynamic Host Configuration Protocol (DHCP), broadband, and VoIP packets: 0/4/0 Forwarding cable modem (CM) management and VoD packets: 0/5/0

Procedure

Step 1 Create an S-VLAN.

The S-VLAN is a user-side service VLAN between the optical line terminal (OLT) and the D-CMTS. The OLT works in Layer 3 forwarding mode.

```
huawei(config)#vlan 100 smart
```

Step 2 Create a CM S-VLAN.

The CM S-VLAN identifies a CM service flow. After the CM S-VLAN is configured, the OLT automatically creates a CM service flow when the CM goes online.

NOTE

- The **cable service-vlan** *vlanid* command is used to configure a global S-VLAN for CM services. After the configuration, all CM services of the D-CMTSs connected to the same OLT use the same VLAN. When the number of IP address segments planned for an OLT is less than eight, this command is recommended.
- The **cable service-vlan** *vlanid frameid/slotid* command is used to configure an S-VLAN for CM services on a specified D-CMTS. After the configuration, the D-CMTS does not use the global S-VLAN. When the number of IP address segments planned for an OLT is greater than eight, this command is recommended.

```
huawei(config)#cable service-vlan 100
  Info: The new service VLAN will take effect after the CM is restarted, are you
 sure to modify? (y/n)[n]:y
```

----End

15.3.1.10 Configuring the DOCSIS VoD Service

A cable modem (CM) connects to a distributed cable modem termination system (D-CMTS) through a cable and provides the DOCSIS VoD service for users.

Context

All home services use a service VLAN (S-VLAN) and the S-VLAN is globally configured. If the S-VLAN has been configured for other home services, use the S-VLAN for the VoD service.

Data Plan

Table 15-15 Data plan for the VoD service

Item	Data
VLAN	ID of the VoD S-VLAN: 100; type of the VLAN: smart

Copyright © Huawei Technologies Co., Ltd.

Item	Data
Uplink ports	Forwarding Dynamic Host Configuration Protocol (DHCP), broadband, and VoIP packets: 0/4/0 Forwarding cable modem (CM) management, VoD, and multicast packets: 0/5/0

Procedure

Step 1 Create an S-VLAN.

The S-VLAN is a user-side service VLAN between the optical line terminal (OLT) and the D-CMTS. The OLT works in Layer 3 forwarding mode.

```
huawei(config)#vlan 100 smart
```

Step 2 Create a CM S-VLAN.

The CM S-VLAN identifies a CM service flow. After the CM S-VLAN is configured, the OLT automatically creates a CM service flow when the CM goes online.

NOTE

- The **cable service-vlan** *vlanid* command is used to configure a global S-VLAN for CM services. After the configuration, all CM services of the D-CMTSs connected to the same OLT use the same VLAN. When the number of IP address segments planned for an OLT is less than eight, this command is recommended.
- The **cable service-vlan** *vlanid frameid/slotid* command is used to configure an S-VLAN for CM services on a specified D-CMTS. After the configuration, the D-CMTS does not use the global S-VLAN. When the number of IP address segments planned for an OLT is greater than eight, this command is recommended.

```
huawei(config)#cable service-vlan 100
  Info: The new service VLAN will take effect after the CM is restarted, are you
 sure to modify? (y/n)[n]:y
```

----End

15.3.1.11 Configuring the EQAM VoD Service

If the MA5633 is equipped with a built-in EQAM module, the MA5633 sets idle downstream DOCSIS channels as EQAM channels to transmit VoD data.

Prerequisites

The MA5633 supports built-in EQAM.

Context

In multiservice operator (MSO)-oriented solutions, both HFC networks and STBs use the broadcast television QAM technology and support only RF signals.

Video data is encapsulated into IP and UDP packet headers that are transmitted on IP networks, which cannot be transmitted on HFC networks. To transmit the video data on HFC networks, the video data must be modulated into RF signals using the EQAM module.

Copyright © Huawei Technologies Co., Ltd.

Video data transmission on HFC networks uses existing CATV coaxial cables on the HFC networks, thereby reducing network deployment costs.

Data Plan

Table 15-16 Data plan for the VoD service

Item	Data
EQAM IP address	10.10.10.10
VLAN	ID of the VoD S-VLAN: 50; type of the VLAN: smart
Uplink port	Forwarding CM management, VoD, and multicast packets: 0/5/0
EQAM channel ID	13-16
Modulation mode	QAM 64
Symbol rate	6.875
UDP port number	501-514

Procedure

Step 1 Use a cable initialization profile to configure RF port parameters.

```
huawei(config)#interface cable init-template
huawei(config-cable-init-template)#cable downstream 13 frequency 115.0 modulation
qam64 enable channel-mode eqam symbol-rate 6.875
huawei(config-cable-init-template)#cable downstream 14 frequency 123.00 modulation
qam64 enable channel-mode eqam symbol-rate 6.875
huawei(config-cable-init-template)#cable downstream 15 frequency 131.00 modulation
qam64 enable channel-mode eqam symbol-rate 6.875
huawei(config-cable-init-template)#cable downstream 16 frequency 139.00 modulation
qam64 enable channel-mode eqam symbol-rate 6.875
huawei(config-cable-init-template)#quit
```

Step 2 Configure a video profile.

A video profile contains all video mappings on an EQAM module and supports batch video mapping configurations. This facilitates video mapping configuration and management.

```
huawei(config)#cable eqam video profile name vod1
huawei(config-eqam-video-profile-vod1)#mapping index 1 type spts udp-port 501
output-program 1 pmtpid 32 channel 13
huawei(config-eqam-video-profile-vod1)#mapping index 2 type spts udp-port 502
output-program 2 pmtpid 48 channel 13
huawei(config-eqam-video-profile-vod1)#mapping index 3 type spts udp-port 503
output-program 3 pmtpid 64 channel 13
huawei(config-eqam-video-profile-vod1)#mapping index 4 type spts udp-port 504
output-program 4 pmtpid 80 channel 13
huawei(config-eqam-video-profile-vod1)#mapping index 5 type spts udp-port 505
output-program 1 pmtpid 96 channel 14
huawei(config-eqam-video-profile-vod1)#mapping index 6 type spts udp-port 506
output-program 2 pmtpid 112 channel 14
huawei(config-eqam-video-profile-vod1)#mapping index 7 type spts udp-port 507
output-program 3 pmtpid 128 channel 14
huawei(config-eqam-video-profile-vod1)#mapping index 8 type spts udp-port 508
output-program 1 pmtpid 160 channel 15
```


Copyright © Huawei Technologies Co., Ltd.

```
huawei(config-eqam-video-profile-vod1)#mapping index 9 type spts udp-port 509
output-program 2 pmtpid 176 channel 15
huawei(config-eqam-video-profile-vod1)#mapping index 10 type spts udp-port 510
output-program 1 pmtpid 224 channel 16
huawei(config-eqam-video-profile-vod1)#mapping index 11 type spts udp-port 511
output-program 2 pmtpid 240 channel 16
huawei(config-eqam-video-profile-vod1)#mapping index 12 type spts udp-port 512
output-program 3 pmtpid 256 channel 16
huawei(config-eqam-video-profile-vod1)#mapping index 13 type spts udp-port 513
output-program 4 pmtpid 272 channel 16
huawei(config-eqam-video-profile-vod1)#mapping index 14 type spts udp-port 514
output-program 5 pmtpid 288 channel 16
huawei(config-eqam-video-profile-vod1)#quit
```

NOTE

To configure video mappings in batches, do as follows:

```
huawei(config)#cable eqam video profile name vod1
huawei(config-eqam-video-profile-vod1)#mapping index 1 type spTS udp-port 501
output-program 1 pmtpid 32 chan
nel 13 number 4 increment output-program 1 pmtpid 32 udp-port 1
huawei(config-eqam-video-profile-vod1)#mapping index 5 type spts udp-port 505
output-program 1 pmtpid 96 chan
nel 14 number 3 increment output-program 1 pmtpid 32 udp-port 1
huawei(config-eqam-video-profile-vod1)#mapping index 8 type spts udp-port 508
output-program 1 pmtpid 160 chan
nel 15 number 2 increment output-program 1 pmtpid 32 udp-port 1
huawei(config-eqam-video-profile-vod1)#mapping index 10 type spts udp-port 510
output-program 1 pmtpid 224 chan
nel 16 number 5 increment output-program 1 pmtpid 32 udp-port 1
```

Step 3 Configure the VoD S-VLAN.

VLAN 50 is the S-VLAN that functions between the OLT and the MA5633. The OLT works in Layer 3 forwarding mode.

```
huawei(config)#vlan 50 smart
huawei(config)#port vlan 50 0/5 0
```

Step 4 Configure a video domain.

A video domain defines the relationships between an EQAM module and an EQAM IP address, and between the S-VLAN used for video data forwarding on an EQAM module, the EQAM module, and a video profile. This facilitates data management.

```
huawei(config)#cable eqam video domain huawei
huawei(config-eqam-domain-huawei)#local ip 10.10.10.10 vlan 50
huawei(config-eqam-domain-huawei)#bind video profile name vod1 1/1/0
huawei(config-eqam-domain-huawei)#quit
```

----End

Result

The MA5633 supports packet statistics query. Based on the statistical results, you can determine whether users can order programs and whether packet loss occurs in program transmitting.

- Run the **display cable eqam video stream** command to check the TS status. If the status is **online**, the TS is functional.
- Run the **display cable eqam video statistics input** command to query packet statistics and network jitter of a TS on the video service input end.

  Check whether the program ordered by a user has been sent to the MA5633. If the program has been sent to the MA5633, check whether the program traffic is normal.

Copyright © Huawei Technologies Co., Ltd.

- Run the **display cable eqam video statistics output** command to query packet statistics of a TS on the video service output end.

  Check whether the TS contains the ordered program, whether the program has been sent to the STB, and whether the TS traffic is normal.

15.3.1.12 Configuring the BTV Service

A cable modem (CM) connects to a distributed cable modem termination system (D-CMTS) through a cable and provides the multicast service for users.

Context

All home services use a service VLAN (S-VLAN) and the S-VLAN is globally configured. If the S-VLAN has been configured for other home services, use the S-VLAN for the multicast service.

Data Plan

Table 15-17 Data plan for the multicast service

Item	Data
VLAN	ID of the multicast S-VLAN: 100; type of the VLAN: smart
Uplink ports	Forwarding Dynamic Host Configuration Protocol (DHCP), broadband, and VoIP packets: 0/4/0 Forwarding cable modem (CM) management, VoD, and multicast packets: 0/5/0

Procedure

Step 1 Create an S-VLAN.

The S-VLAN is a user-side service VLAN between the optical line terminal (OLT) and the D-CMTS. The OLT works in Layer 3 forwarding mode.

```
huawei(config)#vlan 100 smart
```

Step 2 Create a CM S-VLAN.

The CM S-VLAN identifies a CM service flow. After the CM S-VLAN is configured, the OLT automatically creates a CM service flow when the CM goes online.

NOTE

- The **cable service-vlan** *vlanid* command is used to configure a global S-VLAN for CM services. After the configuration, all CM services of the D-CMTSs connected to the same OLT use the same VLAN. When the number of IP address segments planned for an OLT is less than eight, this command is recommended.
- The **cable service-vlan** *vlanid frameid/slotid* command is used to configure an S-VLAN for CM services on a specified D-CMTS. After the configuration, the D-CMTS does not use the global S-VLAN. When the number of IP address segments planned for an OLT is greater than eight, this command is recommended.

Copyright © Huawei Technologies Co., Ltd.

```
huawei(config)#cable service-vlan 100
  Info: The new service VLAN will take effect after the CM is restarted, are you
 sure to modify? (y/n)[n]:y
```

Step 3 Configure multicast VLAN 100.

NOTE

This configuration takes effect only after the CMs go online again.

```
huawei(config)#multicast-vlan 100
```

Step 4 Configure the Internet Group Management Protocol (IGMP) version to IGMPv3.

```
huawei(config-mvlan100)#igmp version v3
```

Step 5 Configure a multicast program generation mode.

Multicast programs can be dynamically or statically generated. For the D-CMTS, the multicast programs are dynamically generated.

```
huawei(config-mvlan100)#igmp mode off
  Are you sure to close IGMP? (y/n)[n]:y
huawei(config-mvlan100)#igmp match mode disable
```

Step 6 Configure the multicast uplink port to 0/5/0.

```
huawei(config-mvlan100)#igmp uplink-port 0/5/0
```

Step 7 Configure the IGMP mode to IGMP proxy.

```
huawei(config-mvlan100)#igmp mode proxy
  Are you sure to change IGMP mode?(y/n)[n]:y
huawei(config-mvlan100)#quit
```

Step 8 Bind CM multicast users to the multicast VLAN.

NOTE

This configuration takes effect only after the CMs go online again.

```
huawei(config)#cable multicast-vlan 100
```

Step 9 (Optional) Disable multicast DSID-based forwarding (MDF).

Multicast DSID-based forwarding is defined in data over cable service interface specification (DOCSIS) 3.0, perform this step if the CMs comply with DOCSIS 2.0.

Disable MDF if the CMTS is connected to a CM equipped with a TI chip. Otherse, the CM may go online and offline repeatedly.

```
huawei(config)#cable multicast mdf disable
```

Step 10 (Optional) Configure multicast user authentication.

NOTE

Perform this step if the configuration file on the CM server contains only the multicast rights profile name and the multicast rights must be configured on the D-CMTS.

The following configurations are used as an example to configure multicast user authentication:

- Multicast authentication function: enabled globally
- Maximum number of programs can be ordered if the CM does not match any rights rule: 32
- IP addresses of the multicast programs that can be ordered by multicast users: 225.1.1.1 and 225.1.1.2
- IP address of the multicast server: 192.168.20.11

Copyright © Huawei Technologies Co., Ltd.

- Multicast program priorities: 254 and 255

```
huawei(config)#cable multicast authorization enable max-sessions 32 default-acti
on permit
huawei(config)#cable multicast auth-profile profile-name btv1
huawei(config-multicast-profile-btv1)#rule 1 priority 255 group-ip 225.1.1.1 gro
up-ip-mask 24 src-ip 192.168.20.11 src-ip-mask 24 permit
huawei(config-multicast-profile-btv1)#rule 1 priority 254 group-ip 225.1.1.2 gro
up-ip-mask 24 src-ip 192.168.20.11 src-ip-mask 24 permit
```

Step 11 (Optional) Configure cable multicast version.

```
huawei(config)#cable multicast igmp-version v3
```

----End

15.3.1.13 Configuring the Dynamic PacketCable Service

A cable modem (CM) connects to a distributed cable modem termination system (D-CMTS) through a cable and provides the dynamic PacketCable service for users.

Context

Table 15-18 Data plan for the PacketCable service on the OLT

Item	Data
Uplink port	Forwarding VoIP packets: 0/4/0
VLAN	ID of service VLAN: 100 ID of the common open policy service (COPS) connection VLAN: 1000
IP address for creating a COPS connection to an IP multimedia subsystem (IMS) or a softswitch	192.168.60.3/24 (in the same network segment as the IMS or softswitch or can communicate with the IMS or softswitch)

Procedure

Step 1 Create a service VLAN (S-VLAN).

NOTE

All home services use an S-VLAN and the S-VLAN is globally configured. If the S-VLAN has been configured for other home services, use the S-VLAN in steps **Step 1** and **Step 2**.

The ID of S-VLAN is 100 and the type of the VLAN is smart. The S-VLAN is a user-side service VLAN between the OLT and the D-CMTS. The OLT works in Layer 3 forwarding mode.

```
huawei(config)#vlan 100 smart
```

Step 2 Create a CM S-VLAN.

The CM S-VLAN identifies a CM service flow. After the CM S-VLAN is configured, the OLT automatically creates a CM service flow when the CM goes online.

Copyright © Huawei Technologies Co., Ltd.

NOTE

- The **cable service-vlan** *vlanid* command is used to configure a global S-VLAN for CM services. After the configuration, all CM services of the D-CMTSs connected to the same OLT use the same VLAN. When the number of IP address segments planned for an OLT is less than eight, this command is recommended.
- The **cable service-vlan** *vlanid frameid/slotid* command is used to configure an S-VLAN for CM services on a specified D-CMTS. After the configuration, the D-CMTS does not use the global S-VLAN. When the number of IP address segments planned for an OLT is greater than eight, this command is recommended.

```
huawei(config)#cable service-vlan 100
  Info: The new service VLAN will take effect after the CM is restarted, are you
 sure to modify? (y/n)[n]:y
```

Step 3 Configure the Layer 3 interface for COPS connections.

```
huawei(config)#vlan 1000 smart
huawei(config)#interface vlanif 1000
huawei(config-if-vlanif1000)#ip address 192.168.60.3 24
huawei(config-if-vlanif1000)#quit
huawei(config)#port vlan 1000 0/4 0
```

Step 4 Configure a COPS connection.

The following configurations are used as an example to configure a COPS connection:

- COPS policy enforcement point (PEP) ID: IP address of the Layer 3 interface for the COPS connection
- Transmit and receive buffer for TCP sockets: 12 KB
- Differentiated services code point (DSCP) priority of COPS packets: ef

```
huawei(config)#cops pepid 192.168.60.3
huawei(config)#cops tcp window 12
huawei(config)#cops ip dscp ef
```

Step 5 Configure PacketCable parameters.

PacketCable 1.x parameter settings are as follows:

- Embedded media terminal adapter (EMTA) creating a dynamic media stream: permitted
- Other parameters: default settings

```
huawei(config)#packetcable 1dotx enable
huawei(config)#packetcable authorize common-docsis-mta enable
huawei(config)#packetcable multimedia enable
```

----End

15.3.1.14 Verifying Services

A distributed cable modem termination system (D-CMTS) working as a remote extended frame locates on an optical node. To facilitate service verification, the optical line terminal (OLT) supports multiple remote service verification methods, such as Dynamic Host Configuration Protocol (DHCP) dialup emulation tests. This allows commissioning and configuration engineers to remotely verify services. In addition, this section describes how to verify the home services on site.

Prerequisites

- The OLT is properly connected to the upper-layer network.

Copyright © Huawei Technologies Co., Ltd.

- The DHCP server, Trivial File Transfer Protocol (TFTP) server, and softswitch or IP multimedia subsystem (IMS) have been configured.

Procedure

- Perform a DHCP dialup emulation test.

  In this test, a cable modem (CM) is emulated on the OLT to apply to the DHCP server for an IP address. This checks whether the OLT can communicate with the DHCP server and verifies CM DHCP configurations on the DHCP relay, proxy, and server.

  1. Run the **simulate dhcp start cm** *mac-address* [**option60** *option60*] command to start a DHCP dialup emulation test.

     NOTE

     You can run the **simulate dhcp stop** command to stop the DHCP emulation.
  2. Run the **display simulation dhcp** command to query the results of the DHCP dialup emulation test.
  3. Check whether the **User IP** has obtained an IP address.
- Check the CM status.

  Run the **display cable modem** command to query the CM status in **Status**.

```
huawei(config)#display cable modem  all

-------------------------------------------------------------------------------
-
 Idx   MAC            IP              I/F          Status   Prim  Num Ver  DS
RX
                                                           SID   CPE
Power

-------------------------------------------------------------------------------
-
 1     0023-ED6F-21A3 192.168.1.118   1/1/0/U4     ol-pt    1     0   D2.0
-

-------------------------------------------------------------------------------
-
 Total:
1
 ol: 0, ol-ptd: 0, ol-pt: 1, ol-d: 0, wol: 0, wol-ptd: 0, wol-pt: 0, wol-d:
0,
pol: 0, pol-ptd: 0, pol-pt: 0, pol-d: 0, offline: 0, rej-m: 0, rej-pt: 0, rej-
o:
 0, init: 0, init-rc: 0, DHCP: 0, DHCP-O: 0, DHCP-R: 0, DHCP-C: 0, REG:
0
 Note: 1. Idx is the index of a
CM.
       2. The downstream received power is in the unit of
dBmV.
       3. In status, "ol" means online, "rej" means reject.
```

  The following table lists the CM status and handling suggestions.

Copyright © Huawei Technologies Co., Ltd.

CM Status	Description	Handling Suggestion
init	Indicates that the CM initialization ranging message is received.the CM initialization.	If a CM is always in the ranging state, the ranging fails. Then check radio frequency (RF) line indicators and detect line faults.
init-rc	Indicates that the CM initialization ranging is complete.	No action is required. The ranging of the CM is complete.
DHCP	Indicates that the DHCP discovery from the CM is received.	If a CM initiates a DHCP request but does not obtain an IP address, check the DHCP server, routing between the OLT and the DHCP server, and DHCP server parameter settings.
● DHCP-O ● DHCP-R ● DHCP-C	● DHCP-O: indicates that the offer from the DHCP server is received. ● DHCP-R: indicates that the DHCP request from the CM is received. ● DHCP-C: indicates that the acknowledge from the DHCP server is received.	The DHCP server has assigned an IP address to the CM and sent configuration file name and IP address of the TFTP or ToD server to the CM using the Option 67 and Option 66 fields (the Option 67 field carries the configuration file name and the Option 66 field carries the IP address of the TFTP or ToD server). If the CM is always in the DHCP-C state, the CM fails to obtain the configuration file. Then check the TFTP server, routing between the OLT and the TFTP server, and TFTP server parameter settings.
REG	Indicates that a registration is started.	If the CM is always in the register state, the CM obtains an incorrect configuration file. Then change the configuration file.

Copyright © Huawei Technologies Co., Ltd.

CM Status	Description	Handling Suggestion
● ol ● ol-pt ● ol-ptd ● ol-d ● wol ● wol-pt ● wol-ptd ● wol-d ● pol ● pol-pt ● pol-ptd	● ol: indicates that the CM is online. (valid only for CMs complying with DOCSIS 2.0) ● ol-pt: indicates that the CM is online and passes the BPI authentication. (valid only for CMs complying with DOCSIS 2.0) ● ol-ptd: indicates that the CM is online and passes the BPI authentication, and NetAccessEnable is disabled. (valid only for CMs complying with DOCSIS 2.0) ● ol-d: indicates that the CM is online and NetAccessEnable is disabled. (valid only for CMs complying with DOCSIS 2.0) ● wol: indicates that the CM is online and all channels bound to the CM are available. (valid only for CMs complying with DOCSIS 3.0) ● wol-pt: indicates that the CM is online and passes the BPI authentication, and all channels bound to the CM are available. (valid only for CMs complying with DOCSIS 3.0) ● wol-ptd: indicates that the CM is online and passes the BPI authentication, NetAccessEnable is disabled, and all channels bound to the CM are available. (valid only for CMs complying with DOCSIS 3.0) ● wol-d: indicates that the CM is online, NetAccessEnable is disabled, and all channels bound to the CM are available. (valid only for CMs complying with DOCSIS 3.0) ● pol: indicates that the CM is online and some channels	No action is required. The status indicates that the CM has registered

Copyright © Huawei Technologies Co., Ltd.

CM Status	Description	Handling Suggestion
● pol-d	bound to the CM are available. (valid only for CMs complying with DOCSIS 3.0) ● pol-pt: indicates that the CM is online and passes the BPI authentication, and some channels bound to the CM are available. (valid only for CMs complying with DOCSIS 3.0) ● pol-ptd: indicates that the CM is online and passes the BPI authentication, NetAccessEnable is disabled, and some channels bound to the CM are available. (valid only for CMs complying with DOCSIS 3.0) ● pol-d: indicates that the CM is online, NetAccessEnable is disabled, and some channels bound to the CM are available. (valid only for CMs complying with DOCSIS 3.0)	with the OLT and can correctly transmit and receive services.
offline	Indicates the offline status.	If the CM is in the offline state, check the power status, noise, and channel frequency of the CM.
● rej-m ● rej-pt ● rej-o	● rej-m: indicates that the MIC verification fails. ● rej-pt: indicates that the BPI authentication fails. ● rej-o: indicates that the authentication reject due to other reasons.	If the CM is in the reject state, no service flow can be created. Then check the CM authentication and CM message integrity check (MIC), and check whether class of service (COS) parameters specified in the CM configuration file are supported by the OLT.

- Verify that home services can be provisioned.
  1. After the CM is installed at a user home and commissioned, the user can watch TV programs.
  2. After the high-speed Internet (HSI) service is provisioned, the user can access the Internet from a PC.
  3. After the VoD service is provisioned, the user can order programs.
  4. After the VoIP service is provisioned, the user can make and receive phone calls.

Copyright © Huawei Technologies Co., Ltd.

5. After the multicast service is provisioned, the user can watch ordered multicast programs.

----End

15.3.2 L2VPN Enterprise Service Networking

In L2VPN enterprise service networking, a distributed cable modem termination system (D-CMTS) connects to cable modems (CMs) through radio frequency (RF) ports, and the CMs connect to switches or routers to provide the L2VPN service for users. This section describes how to configure the optical line terminal (OLT) to provision the L2VPN service.

NOTE

Configuration procedures are the same for IPv6 and IPv4 networks except in "Configure Dynamic Host Configuration Protocol (DHCP) relay" and "Configure a route".

15.3.2.1 Service Requirements and Usage Scenario

Service Requirements

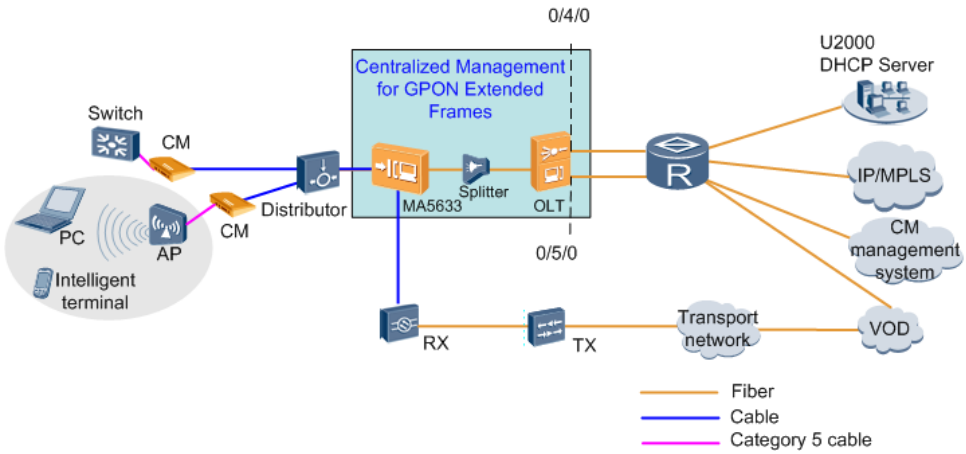
An enterprise requires the provisioning of the L2VPN service.

Usage Scenario

As shown in **Figure 15-10**, an MA5633 is deployed on an optical node and cable modems (CMs) are deployed at enterprises. The CMs connect to radio frequency (RF) ports on the MA5633 through cables.

- A CM provides the enterprise service through a switch, which connects to enterprise users.
- Enterprise users access the Internet through Dynamic Host Configuration Protocol (DHCP) dialup.
- The MA5633 works as a GPON remote extended frame. This reduces MA5633 management and maintenance costs and simplifies configurations.

Figure 15-10 L2VPN enterprise service networking

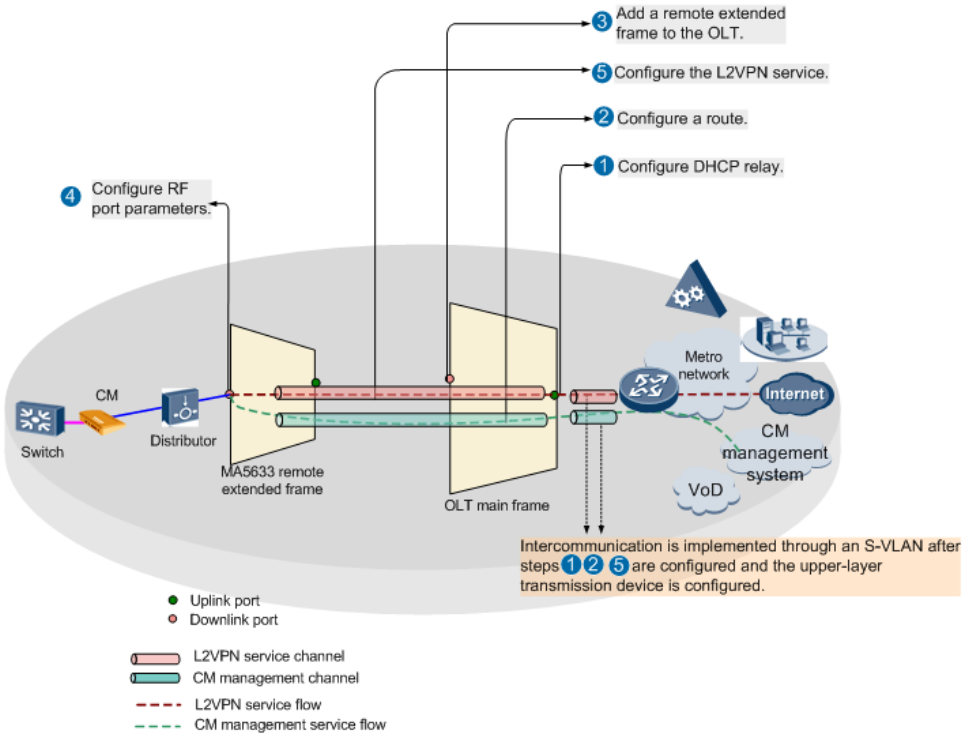


Copyright © Huawei Technologies Co., Ltd.

15.3.2.2 Configuration Process

Figure 15-11 shows the configuration roadmap for the L2VPN service networking.

Figure 15-11 Configuration roadmap for the L2VPN service networking



The following table describes the configuration steps. All configurations are issued from the optical line terminal (OLT).

No.	Step	Description
1	● IPv4: **Configure Dynamic Host Configuration Protocol (DHCP) relay.** ● IPv6: **Configure Dynamic Host Configuration Protocol (DHCP) relay (IPv6).**	This section describes how to configure Dynamic Host Configuration Protocol (DHCP) relay so that cable modems (CMs) can obtain IP addresses in different network segments.
2	● IPv4: **Configure a route.** ● IPv6: **Configure a route (IPv6).**	This section describes how to implement network communication by configuring a route in Layer 3 networking with an optical line terminal (OLT). Through the route, packets are forwarded at Layer 3 between the OLT and its upper-layer devices or servers.

Copyright © Huawei Technologies Co., Ltd.

No.	Step	Description
3	**Add a remote extended frame to the OLT.**	An MA5633 that works as a remote extended frame connects to a port on a cascading board of an optical line terminal (OLT). You can configure the remote extended frame only after adding it to the OLT.
4	**Configure radio frequency (RF) port parameters.**	Radio frequency (RF) port parameters define the frequency spectrum range for signal transmission and modulation mode. The configuration of RF port parameters implements data service transmission over cables. RF port parameters can be configured using either of the following methods: ● Use a cable initialization profile to configure the parameters. ● Customize the parameters in cable mode.
5	**Configure the L2VPN service.**	In the upstream direction, a cable modem (CM) connects to a distributed cable modem termination system (D-CMTS) through a cable. In the downstream direction, the CM connects to a switch to provide the L2VPN enterprise service to the users connected to the switch.
6	**Verify the configured service.**	An OLT supports multiple remote service verification methods. This allows commissioning and configuration engineers to remotely verify services. 1. A DHCP dialup emulation test checks whether the OLT can communicate with the DHCP server and verifies CM DHCP configurations on the DHCP relay, proxy, and server. 2. The status of a CM can be queried. Based on the information, you can determine whether the CM is online.

15.3.2.3 Configuring DHCP Relay

This section describes how to configure Dynamic Host Configuration Protocol (DHCP) relay so that cable modems (CMs) can obtain IP addresses in different network segments.

Copyright © Huawei Technologies Co., Ltd.

Prerequisites

The upper-layer router, DHCP server, and Trivial File Transfer Protocol (TFTP) server of an optical line terminal (OLT) have been configured.

Data Plan

Table 15-19 DHCP data plan for the OLT

Item	Data
VLAN	ID of the CM management S-VLAN: 200; type of the VLAN: smart
DHCP server group parameters	IP address of the DHCP domain gateway for CMs: 10.10.224.1; domain name: docsis

Table 15-20 Data plan for the upper-layer devices of the OLT

Item	IP Address
Layer 3 interfaces connecting the router to the OLT	● Forwarding DHCP and broadband packets: 11.11.11.11 ● Forwarding CM management packets: 11.11.12.11
IP address of the DHCP server	DHCP server assigning IP addresses to CMs and media terminal adapters (MTAs): 192.168.10.10-192.168.10.11

Procedure

Step 1 Set the IP address of the VLAN Layer 3 interface.

```
huawei(config)#vlan 100 smart
huawei(config)#interface vlanif 100
huawei(config-if-vlanif100)#ip address 10.10.224.1 255.255.255.0     //Set the IP address of the DHCP domain gateway for CMs.
huawei(config-if-vlanif100)#quit
```

Step 2 Configure the working mode of the DHCP relay to Layer 3 Option 60.

In DHCP Option 60 mode, a DHCP server group is selected according to the Option 60 domain name in DHCP packets. Users in this mode are identified by domain information of packets, which differentiates various service types in a VLAN. Ensure that the Option 60 domain name and the DHCP server group bound to the Option 60 domain name are configured beforehand.

```
huawei(config)#dhcp mode layer-3 Option60
  Several minutes may be required and no action can be taken during this period
  Are you sure to perform this operation? (y/n)[n]: y
```

Step 3 Set the IP addresses of the servers in a DHCP server group.

```
huawei(config)#dhcp-server 0 ip 192.168.10.10 192.168.10.11    //Configure DHCP server group 0 to assign IP addresses to CMs.
```


Copyright © Huawei Technologies Co., Ltd.

Step 4 Create a DHCP Option 60 domain.

```
huawei(config)#dhcp domain docsis   //Create Option 60 domain name docsis for CMs.
huawei(config-dhcp-domain-docsis)#dhcp-server 0 vlan 100       //Bind DHCP server
group 0 to the DHCP domain where the CMs locate. After the configuration, the CMs
in the DHCP domain are corresponded to DHCP server group 0.
huawei(config-dhcp-domain-docsis)#quit
```

Step 5 Set the IP address of the gateway for the DHCP domain.

```
huawei(config)#interface vlanif 100
huawei(config-if-vlanif100)#dhcp domain docsis gateway 10.10.224.1    //Set the IP
address of the gateway for the CM domain to 10.10.224.1.
huawei(config-if-vlanif100)#quit
```

----End

15.3.2.4 Configuring a Route

This section describes how to implement network communication by configuring a route in Layer 3 networking with an optical line terminal (OLT). Through the route, packets are forwarded at Layer 3 between the OLT and its upper-layer devices or servers.

Prerequisites

The upper-layer router of an OLT has been configured.

Data Plan

Table 15-21 Data plan for the Layer 3 interfaces on the network side

Item	IP Address
Layer 3 interfaces on the OLT network side	Forwarding Dynamic Host Configuration Protocol (DHCP) packets: ● VLAN ID: 2004 ● Port number: 0/4/0 ● IP address: 11.11.11.10/24 Forwarding cable modem (CM) management packets: ● VLAN ID: 2005 ● Port number: 0/5/0 ● IP address: 11.11.12.10/24
Layer 3 interfaces connecting the router to the OLT	● Forwarding DHCP packets: 11.11.11.11 ● Forwarding CM management packets: 11.11.12.11
Upper-layer servers of the OLT	● DHCP server assigning IP addresses to CMs and media terminal adapters (MTAs): 192.168.10.10-192.168.10.11 ● CM management system: 192.168.20.1

Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Create Layer 3 VLAN interfaces on the network side.

1. Create VLANs and configure their uplink ports.
   - VLAN 2004 is of the smart VLAN type and used for forwarding DHCP packets. Add uplink port 0/4/0 to VLAN 2004.
   - VLAN 2005 is of the smart VLAN type and used for forwarding CM management packets. Add uplink port 0/5/0 to VLAN 2005.

```
huawei(config)#vlan 2004 to 2006 smart
huawei(config)#port vlan 2004 0/4 0
huawei(config)#port vlan 2005 0/5 0
```

2. (Optional) Create native VLANs for Ethernet outbound ports.

   Packets between the OLT and its upper-layer router are forwarded at Layer 3 and no VLAN information is required. The created native VLANs remove VLAN tags from the packets transmitted out of Ethernet ports.

```
huawei(config)#interface eth 0/4
huawei(config-if-eth-0/4)#native-vlan 0 vlan 2004    //Remove VLAN tags from
the packets transmitted out of the 0/4/0 port.
huawei(config-if-eth-0/4)#quit
huawei(config)#interface eth 0/5
huawei(config-if-eth-0/5)#native-vlan 0 vlan 2005    //Remove VLAN tags from
the packets transmitted out of the 0/5/0 port.
huawei(config-if-eth-0/5)#quit
```

3. Create Layer 3 VLAN interfaces.
   a. Create a Layer 3 interface for VLAN 2004, through which DHCP packets are forwarded.

```
huawei(config)#interface vlanif 2004
huawei(config-if-vlanif2004)#ip address 11.11.11.10 255.255.255.0
huawei(config-if-vlanif2004)#quit
```

   b. Create a Layer 3 interface for VLAN 2005, through which CM management packets are forwarded.

```
huawei(config)#interface vlanif 2005
huawei(config-if-vlanif2005)#ip address 11.11.12.10 255.255.255.0
huawei(config-if-vlanif2005)#quit
```

Step 2 Configure static routes to implement the communication between the OLT and its upper-layer devices.

```
huawei(config)#ip route-static 192.168.20.0 255.255.255.0 11.11.12.11     //CM
management and VoD packets are forwarded through the Layer 3 interface of VLAN
2005.
huawei(config)#ip route-static 192.168.10.0 255.255.255.0 11.11.11.11     //DHCP
packets are forwarded through the Layer 3 interface of VLAN 2004.
```

NOTE

The interconnected router must set static routes and add the routes to dynamic routes.

----End

Result

The OLT can communicate with its upper-layer devices. To check network connectivity between two devices, run the **ping** and **tracert** commands.

Copyright © Huawei Technologies Co., Ltd.

The configured static routes can be queried in an IPv4 routing table by running the **display ip routing-table** command.

15.3.2.5 Configuring DHCP Relay (IPv6)

This section describes how to configure DHCPv6 relay so that CMs can obtain IP addresses in different network segments.

Prerequisites

The upper-layer router, DHCP server, and Trivial File Transfer Protocol (TFTP) server of an OLT have been configured.

Data Plan

Table 15-22 data plan

Configuration Item	Data
Terminal-side of CM	network segment of CM: 2001:0db8:0001::/64
User-side of OLT	IP address of the gateway for the DHCP domain of CMs: 2001:0db8:0001::1/64; domain name: **docsis**
Network-side of OLT	Forwarding DHCP and broadband packets: ● VLAN ID: 2004 ● Port number: 0/4/0 ● IP address: 2001:0db8:0007::12/64 Forwarding CM management packets, multicast packets, and VoD packets: ● VLAN ID: 2005 ● Port number: 0/5/0 ● IP address: 2001:0db8:0008::13/64
Router	● IP address of the Layer 3 interface for forwarding DHCP and broadband packets: 2001:0db8:0007::6/64 ● IP address of the Layer 3 interface for forwarding CM management packets: 2001:0db8:0008::7/64
Server	● IP addresses of DHCP servers: – DHCP server allocating IP addresses for CMs: 2001:0db8:0006::8/64-2001:0db8:0006::9/64 – DHCP server allocating IP addresses for PCs: 2001:0db8:0006::10/64-2001:0db8:0006::11/64 ● IP addresses of the CM management system: 2001:0db8:0011::14/64-2001:0db8:0011::16/64

Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Configure a CM service provisioning mode, which can be IPv6 (preferentially used), APM, or DPM (used for dual-stack service provisioning). Select a mode based on site requirements.

```
huawei(config)#interface cable 1/1/0
huawei(config-if-cable-1/1/0)#cable ip-mode dpm
huawei(config-if-cable-1/1/0)#quit
```

Step 2 Configure the IP address of the VLAN Layer 3 interface.

```
huawei(config)#ipv6      //Enable IPv6 packet forwarding.
huawei(config)#vlan 100
huawei(config)#interface vlanif 100
huawei(config-if-vlanif100)#ipv6 enable     //Enable IPv6 on ports.
huawei(config-if-vlanif100)#undo ipv6 nd ra halt       //enables a router to send
RA messages.
huawei(config-if-vlanif100)#ipv6 nd autoconfig managed-address-flag     //Configure
the state-based auto-configuration address flag bit. The host obtains an IPv6
address using the state-based automatic configuration.
huawei(config-if-vlanif100)#ipv6 address 2001:0db8:0001::1/64     //Configure the
IP address of the gateway for the DHCP domain of CMs.
huawei(config-if-vlanif100)#quit
```

Step 3 Enable duplicate address detect (DAD) proxy, which prevents repeated link local addresses (LLAs) on the user side.

After receiving a DAD packet sent from the user side with destination IP address LLA, the OLT with DAD proxy enabled checks user online information based on the destination IP address and VLAN. If a user with the same IP address in the VLAN has been online, the OLT makes a response and prohibits the new user from going online. Otherwise, the OLT does not make a response.

```
huawei(config)#ipv6 dad proxy enable
huawei(config)#vlan service-profile profile-id 10
huawei(config)#vlan bind service-profile 100 profile-id 10
huawei(config-vlan-srvprof-10)#ipv6 dad proxy enable     //DAD proxy takes effect
after it is enabled at system level and VLAN service profile level.
```

Step 4 Configure the working mode of DHCP relay to Layer 3 Option 16.

Option 16 is an option with code 16 in DHCPv6 packets, which identifies terminal types. In DHCPv6 Option 16 mode, packets select a DHCPv6 server based on the Option 16 domain. Therefore, in DHCPv6 Option 16 mode, packets select a DHCPv6 server based on terminal types.

```
huawei(config)#dhcpv6 mode layer-3 option16
  Several minutes may be required and no action can be taken during this period
  Are you sure to perform this operation? (y/n)[n]: y
```

Step 5 Configure the IP addresses of the servers in a DHCP server group.

```
huawei(config)#dhcpv6-server 0 ipv6 2001:0db8:0006::8/64 2001:0db8:0006::9/64    //
Configure DHCP server group 0 to allocate IP addresses for CMs.
```

Step 6 Create DHCP Option 16 domains.

```
huawei(config)#dhcp domain docsis   //Create Option 16 domain docsis for CMs.
huawei(config-dhcp-domain-docsis)#dhcpv6-server 0 vlan 100      //Bind DHCP server
group 0 to the DHCP domain of CMs. After the configuration, the CMs in this DHCP
domain are mapped to DHCP server group 0.
huawei(config-dhcp-domain-docsis)#quit
```

Step 7 Configure the IP addresses of the gateways for DHCP domains.

```
huawei(config)#interface vlanif 100
huawei(config-if-vlanif100)#dhcpv6 domain docsis gateway 2001:0db8:0001::1/64    //
```


Copyright © Huawei Technologies Co., Ltd.

```
Configure the IP address of the gateway for the DHCP domain of CMs.
huawei(config-if-vlanif100)#quit
```

----End

15.3.2.6 Configuring a Route (IPv6)

This section describes how to implement network communication by configuring a route in Layer 3 networking with an OLT. Through the route, the OLT can forward packets at Layer 3 between the OLT and its upper-layer devices or servers.

Prerequisites

The upper-layer router of the OLT has been configured.

Data Plan

Table 15-23 data plan

Configuration Item	Data
Terminal-side of CM	network segment of CM: 2001:0db8:0001::/64
User-side of OLT	IP address of the gateway for the DHCP domain of CMs: 2001:0db8:0001::1/64; domain name: **docsis**
Network-side of OLT	Forwarding DHCP and broadband packets: ● VLAN ID: 2004 ● Port number: 0/4/0 ● IP address: 2001:0db8:0007::12/64 Forwarding CM management packets, multicast packets, and VoD packets: ● VLAN ID: 2005 ● Port number: 0/5/0 ● IP address: 2001:0db8:0008::13/64
Router	● IP address of the Layer 3 interface for forwarding DHCP and broadband packets: 2001:0db8:0007::6/64 ● IP address of the Layer 3 interface for forwarding CM management packets: 2001:0db8:0008::7/64
Server	● IP addresses of DHCP servers: – DHCP server allocating IP addresses for CMs: 2001:0db8:0006::8/64-2001:0db8:0006::9/64 – DHCP server allocating IP addresses for PCs: 2001:0db8:0006::10/64-2001:0db8:0006::11/64 ● IP addresses of the CM management system: 2001:0db8:0011::14/64-2001:0db8:0011::16/64

Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Create VLAN Layer 3 interfaces on the network side.

1. Create VLANs and add an uplink port to them, respectively.
   - VLAN 2004 used for forwarding DHCP packets is a smart VLAN. Add uplink port 0/4/0 to VLAN 2004.
   - VLAN 2005 used for forwarding CM management packets is a smart VLAN. Add uplink port 0/5/0 to VLAN 2005.

```
huawei(config)#vlan 2004 to 2005 smart
huawei(config)#port vlan 2004 0/4 0
huawei(config)#port vlan 2005 0/5 0
```

2. (Optional) Create native VLANs for Ethernet outbound ports.

   Packets between the OLT and its upper-layer router are forwarded at Layer 3 and no VLAN tag is required. The created native VLANs remove VLAN tags from the packets transmitted out of Ethernet ports.

```
huawei(config)#interface eth 0/4
huawei(config-if-eth-0/4)#native-vlan 0 vlan 2004    //The packets transmitted
out of port 0/4/0 are untagged.
huawei(config-if-eth-0/4)#quit
huawei(config)#interface eth 0/5
huawei(config-if-eth-0/5)#native-vlan 0 vlan 2005    //The packets transmitted
out of port 0/5/0 are untagged.
huawei(config-if-eth-0/5)#quit
```

3. Create VLAN Layer 3 interfaces.
   a. Create the Layer 3 interface of VLAN 2004, through which DHCP packets are forwarded.

```
huawei(config)#interface vlanif 2004
huawei(config-if-vlanif2004)#ipv6 address 2001:0db8:0007::12/64
huawei(config-if-vlanif2004)#quit
```

   b. Create the Layer 3 interface of VLAN 2005, through which CM management packets are forwarded.

```
huawei(config)#interface vlanif 2005
huawei(config-if-vlanif2005)#ipv6 address 2001:0db8:0008::13/64
huawei(config-if-vlanif2005)#quit
```

Step 2 Configure static routes for the communication between the OLT and its upper-layer devices.

```
huawei(config)#ipv6 route-static 2001:0db8:0006::/64 2001:0db8:0008::7/64     //CM
management packets are forwarded through the Layer 3 interface of VLAN 2005.
huawei(config)#ipv6 route-static 2001:0db8:0011::/64 2001:0db8:0007::6/64     //
DHCP packets are forwarded through the Layer 3 interface of VLAN 2004.
```

NOTE

Configure static routes on the router connected to the OLT. In addition, add the static routes to dynamic ones.

----End

Result

The OLT can communicate with its upper-layer devices. To check network connectivity between two devices, run the **ping ipv6** and **tracert ipv6** commands.

The configured static routes can be queried in an IPv6 routing table by running the **display ipv6 routing-table** command.

Copyright © Huawei Technologies Co., Ltd.

15.3.2.7 Adding a Remote Extended Frame to an OLT

An MA5633 that works as a remote extended frame connects to a port on a cascading board of an optical line terminal (OLT). You can configure the remote extended frame only after adding it to the OLT.

Prerequisites

The MA5633 management policy is set to **extend-frame**. To do so, run the **sysman centralized-mgmt primary** command.

Context

A GPON remote extended frame is added to an OLT in the following two steps: Add the MA5633 to the OLT as a GPON optical network unit (ONU). Then add the MA5633 to the OLT as a GPON remote extended frame.

You can use either of the methods listed in the following table to add a remote extended frame to an OLT based on site requirements.

Table 15-24 Methods of adding a remote extended frame to an OLT

Method	Usage Scenario	Remarks
Add a remote extended frame in offline mode.	A carrier has planned all remote extended frame IDs together and the remote extended frames must be deployed one by one. This method facilitates remote extended frame management.	1. You have obtained the serial number (SN) of the remote extended frame. 2. The remote extended frame ID has been planned.
Add an automatically discovered remote extended frame.	A great number of remote extended frames need to be deployed. This method reduces manual configurations.	1. You do not know the SN of the remote extended frame. 2. The remote extended frame ID does not need to be planned.

Copyright © Huawei Technologies Co., Ltd.

Data Plan

Table 15-25 Data plan

Item	Data
GPON cascading board	Board: H801GPMD Port ID: 0/3/1 Remote extended frame ID: 1 Remote extended frame authentication mode: SN Remote extended frame SN: 48575443E6D8B541 **NOTE** The OLT uses the MA5603T as an example. The configuration method is the same for other OLTs. The only difference lies in slot IDs.
Dynamic bandwidth allocation (DBA)	Profile: default Type: type4 Maximum bandwidth: 1000 Mbit/s
Line profile	Profile: default GPON encapsulation mode (GEM) port ID: 0 (fixed port in centralized management mode) Transmission container (T-CONT) ID: 1 (fixed T-CONT in centralized management mode)
MA5633 management mode	extend-frame

Procedure

- Add a remote extended frame in offline mode.

  ```
  huawei(config)#frame add 1 MA5633 extending-port 0/3/1 sn 48575443E6D8B541
  ```

  NOTE

  When running the **frame add** command to add a remote extended frame in offline mode, the OLT automatically allocates a temporary SN for the remote extended frame. Therefore, you do not need to specify the SN of the remote extended frame. After obtaining the SN of the remote extended frame, run the **frame bind** command to add the binding relationship between the SN and the remote extended frame to the OLT. Then the remote extended frame is added.

- Add an automatically discovered remote extended frame.

  The OLT supports the adding of an automatically discovered GPON remote extended frame. This function does not require manual confirmation, thereby simplifying the remote extended frame registration and adding flow.

  ```
  huawei(config)#interface gpon 0/3
  huawei(config-if-gpon-0/3)#port 1 ont-auto-find enable
  huawei(config-if-gpon-0/3)#quit
  ```

----End

Copyright © Huawei Technologies Co., Ltd.

Result

The remote extended frame is online.

After adding the remote extended frame, run the **display frame info** command to query the status of the remote extended frame. Ensure that **Online state** is **online** and **State** is **normal**.

```
huawei(config)#display frame info 1
  ---------------------------------------------------------------------------
  Type:           MA5633
  State:          Normal
  Desc:           MA5633_1_extending_0/3/1/1
  Hardware:       MA5633
  Extend type:    GPON
  Extending port: 0 /3 /1
  ONT ID:         1
  ONT SN:         48575443E6D8B541
  Extended port:  1 /0 /1
  Online state:   Online
  Optical-receiver: Offline
  ---------------------------------------------------------------------------
```

Follow-up Procedure

If the remote extended frame cannot be discovered, follow the troubleshooting suggestions listed in the following table to rectify faults.

Possible Cause	Troubleshooting Suggestion
The MA5633 automatic discovery function is disabled.	In GPON mode, run the **port ont-auto-find** command to enable the MA5633 automatic discovery function on GPON ports.
The MA5633 works as a standalone NE and cannot work as a remote extended frame.	Replace the MA5633 with the one that works as a remote extended frame.
The MA5633 management policy is set to **stand-alone** on the OLT.	Run the **sysman centralized-mgmt primary** command to configure the MA5633 management policy to **extend-frame**.
The number of remote extended frames on the OLT has reached the threshold.	Run the **frame delete** command to delete a remote extended frame that is no longer used from the OLT.

15.3.2.8 Configuring RF Port Parameters

Radio frequency (RF) port parameters define the frequency spectrum range for signal transmission and modulation mode. The configuration of RF port parameters implements data service transmission over cables.

Context

You can use either of the methods listed in the following table to configure RF port parameters based on site requirements.

Copyright © Huawei Technologies Co., Ltd.

Table 15-26 Methods of configuring RF port parameters

Method	Usage Scenario	Remarks
Use a cable initialization profile to configure RF port parameters.	A carrier needs to deploy remote extended frames in batches. This method reduces data configuration for remote extended frames, thereby improving service provisioning efficiency. Configure the RF parameter profile for the remote extended frames on the optical line terminal (OLT). After the remote extended frames are powered on and added to the OLT, the OLT automatically issues the RF parameter profile to the remote extended frames, without requiring any software configuration. **NOTE** After the cable initialization profile is configured, a remote extended frame uses the RF port parameters configured in the profile after going online, regardless of whether the remote extended frame in added in offline mode or automatically discovered by the OLT.	● If the RF port parameters are the same for all the remote extended frames to be deployed in batches, use the cable initialization profile to configure the parameters. ● If the RF port parameters are basically the same for all the remote extended frames to be deployed in batches, use the cable initialization profile to configure the parameters. Then modify parameter settings in customized cable configuration mode.
Customize RF port parameters in cable mode.	Requires differentiated plans and configurations for RF port parameters of remote extended frames and the remote extended frames must be configured one by one.	If the RF port parameters are greatly different for the remote extended frames to be deployed in batches, use this method to configure the parameters.

Data Plan

Table 15-27 Data plan for RF port parameters

Item	Data
RF port	1/1/0

Copyright © Huawei Technologies Co., Ltd.

Item	Data
Upstream channels	● IDs: 1-4 ● Type: European standard (default channel type) ● ID of the upstream channel modulation profile: 1 (by default) ● Channel central frequency (MHz): 29.8, 42.60, 49.00, and 55.4
Downstream channels	● IDs: 1-16 ● Type: European standard (default channel type) ● Channel central frequency (MHz): 602.00, 610.00, 618.00, ..., and 722.00

Procedure

- Use a cable initialization profile to configure RF port parameters.
  1. Configure the frequency spectrum range and channel type.

     In this example, the channel is of the European type. To change the type to North American, run the **cable** command.
  2. Configure RF port parameters for upstream channels and activate the upstream channels.

Parameter	Description
frequency and **channel-width**	A central frequency and a frequency bandwidth determine a frequency range, within which packets are transmitted. For example, the central frequency of a European channel is 55 MHz and the frequency bandwidth is 6400 kHz. Then the frequency range of the channel is 51.8-58.2 MHz.
modulation-profile	An upstream channel modulation profile defines parameters for processing the signals transmitted over the upstream channel. You do not need to configure an upstream channel modulation profile generally. Ports automatically bind to profile 1 by default.

The following configurations are used as an example to configure RF parameters for upstream channels:

- Number of upstream channels: 4
- Frequency bandwidth of the channels: 3.2 MHz (default value)

```
huawei(config)#interface cable init-template
huawei(config-cable-init-template)#cable upstream 1 frequency 29.8 enable
huawei(config-cable-init-template)#cable upstream 2 frequency 42.60
```


Copyright © Huawei Technologies Co., Ltd.

```
enable
huawei(config-cable-init-template)#cable upstream 3 frequency 49.00
enable
huawei(config-cable-init-template)#cable upstream 4 frequency 55.40
enable
```

3. Configure RF port parameters for downstream channels and activate the downstream channels.

Parameter	Description
modulation	A greater modulation mode value for downstream channels results in a higher channel bandwidth but weaker anti-interference capability. Therefore, configure the modulation mode based on site requirements. The default modulation mode is QAM256. This example uses the default setting.

The following configuration is used as an example to configure RF parameters for downstream channels: A total of 16 downstream channels have been purchased.

```
huawei(config-cable-init-template)#cable downstream 1 frequency 602.00
enable
huawei(config-cable-init-template)#cable downstream 2 frequency 610.00
enable
huawei(config-cable-init-template)#cable downstream 3 frequency 618.00
enable
huawei(config-cable-init-template)#cable downstream 4 frequency 626.00
enable
huawei(config-cable-init-template)#cable downstream 5 frequency 634.00
enable
huawei(config-cable-init-template)#cable downstream 6 frequency 642.00
enable
huawei(config-cable-init-template)#cable downstream 7 frequency 650.00
enable
huawei(config-cable-init-template)#cable downstream 8 frequency 658.00
enable
huawei(config-cable-init-template)#cable downstream 9 frequency 666.00
enable
huawei(config-cable-init-template)#cable downstream 10 frequency 674.00
enable
huawei(config-cable-init-template)#cable downstream 11 frequency 682.00
enable
huawei(config-cable-init-template)#cable downstream 12 frequency 690.00
enable
huawei(config-cable-init-template)#cable downstream 13 frequency 698.00
enable
huawei(config-cable-init-template)#cable downstream 14 frequency 706.00
enable
huawei(config-cable-init-template)#cable downstream 15 frequency 714.00
enable
huawei(config-cable-init-template)#cable downstream 16 frequency 722.00
enable
```

- Customize the RF port parameters in cable mode.

  NOTE

  The configuration is complete if you have configured the RF port parameters using a cable initialization profile. For details, see **Use a cable initialization profile to configure RF port parameters**. Perform this operation if you need to customize the RF port parameters of a remote extended frame.

Copyright © Huawei Technologies Co., Ltd.

1. Configure RF port parameters for upstream channels and activate the upstream channels.

```
huawei(config)#interface cable 1/1/0
huawei(config-if-cable-1/1/0)#cable upstream 1 frequency 29.8 enable
huawei(config-if-cable-1/1/0)#cable upstream 2 frequency 42.60 enable
huawei(config-if-cable-1/1/0)#cable upstream 3 frequency 49.00 enable
huawei(config-if-cable-1/1/0)#cable upstream 4 frequency 55.40 enable
```

2. Configure RF port parameters for downstream channels and activate the downstream channels.

```
huawei(config-if-cable-1/1/0)#cable downstream 1 frequency 602.00 enable
huawei(config-if-cable-1/1/0)#cable downstream 2 frequency 610.00 enable
huawei(config-if-cable-1/1/0)#cable downstream 3 frequency 618.00 enable
huawei(config-if-cable-1/1/0)#cable downstream 4 frequency 626.00 enable
huawei(config-if-cable-1/1/0)#cable downstream 5 frequency 634.00 enable
huawei(config-if-cable-1/1/0)#cable downstream 6 frequency 642.00 enable
huawei(config-if-cable-1/1/0)#cable downstream 7 frequency 650.00 enable
huawei(config-if-cable-1/1/0)#cable downstream 8 frequency 658.00 enable
huawei(config-if-cable-1/1/0)#cable downstream 9 frequency 666.00 enable
huawei(config-if-cable-1/1/0)#cable downstream 10 frequency 674.00 enable
huawei(config-if-cable-1/1/0)#cable downstream 11 frequency 682.00 enable
huawei(config-if-cable-1/1/0)#cable downstream 12 frequency 690.00 enable
huawei(config-if-cable-1/1/0)#cable downstream 13 frequency 698.00 enable
huawei(config-if-cable-1/1/0)#cable downstream 14 frequency 706.00 enable
huawei(config-if-cable-1/1/0)#cable downstream 15 frequency 714.00 enable
huawei(config-if-cable-1/1/0)#cable downstream 16 frequency 722.00 enable
```

----End

Result

1. The transmit power of the downstream channels meets site requirements.

   Run the **display cable downstream** *frameid/slotid/portid* { **all** | *channel-id* } **status** command to check whether the RF port parameters meet site requirements.

2. The signal-to-noise (SNR) ratio of the upstream channels meets site requirements.

   Run the **display cable signal quality** [*frameid/slotid/portid* [**upstream** *channel-id*]] command to check whether the RF port parameters meet site requirements. A greater SNR ratio results in better signal quality. The recommended SNR ratio is greater than 30 dB.

15.3.2.9 Configuring the L2VPN Enterprise Service

In the upstream direction, a cable modem (CM) connects to a distributed cable modem termination system (D-CMTS) through a cable. In the downstream direction, the CM connects to a switch to provide the L2VPN enterprise service to the users connected to the switch.

Context

An L2VPN S-VLAN can be configured through a CM configuration file or commands. Only one mode is used each time generally. If both modes are used, the S-VLAN configuration through commands preferentially takes effect on the system when the CM goes online.

- S-VLAN configuration through a CM configuration file: Run the **vlan** command to add a CM S-VLAN and run the **port vlan** command to add the uplink port for the CM to the S-VLAN. The L2VPN S-VLAN is specified in the CM configuration file. When the CM goes online, the system obtains the L2VPN S-VLAN from the CM configuration file and automatically creates L2VPN service flows.

Copyright © Huawei Technologies Co., Ltd.

- S-VLAN configuration through commands: Manually configure the L2VPN S-VLAN on the system. For details, see the following procedure.

Data Plan

Table 15-28 Data plan for the L2VPN service

Item	Data
VLAN	ID of the L2VPN S-VLAN: 200; type of the VLAN: smart
Uplink ports	Port forwarding Dynamic Host Configuration Protocol (DHCP) and broadband packets: 0/4/0 Port forwarding CM management packets: 0/5/0

Procedure

Step 1 Create an L2VPN S-VLAN and add the uplink port to it.

The ID of the L2VPN S-VLAN is 200 and the type of the VLAN is smart. Uplink port 0/4/0 is added to S-VLAN 200.

When the L2VPN S-VLAN is configured through commands, the ID of the L2VPN VLAN is 200 for the CM with MAC address 0000-0000-1111 connected to port 1/1/0.

- To configure the L2VPN S-VLAN through a CM configuration file, run the following commands:

```
huawei(config)#vlan 200 smart
huawei(config)#port vlan 200 0/4 0
```

- To configure the L2VPN S-VLAN through commands, run the following commands:

```
huawei(config)#vlan 200 smart
huawei(config)#cable l2vpn dot1q 1/1/0 cm 0000-0000-1111 200
huawei(config)#port vlan 200 0/4 0
```

Step 2 Configure a VLAN service profile and set the DHCP forwarding mode for VLAN 200 to Layer 2 forwarding.

```
huawei(config)#vlan service-profile profile-name l2vpn
huawei(config-vlan-srvprof-1)#dhcp mode layer-2
huawei(config-vlan-srvprof-1)#commit
huawei(config-vlan-srvprof-1)#quit
huawei(config)#vlan bind service-profile 200 profile-name l2vpn
```

----End

15.3.2.10 Verifying Services

A distributed cable modem termination system (D-CMTS) working as a remote extended frame locates on an optical node. To facilitate service verification, the optical line terminal (OLT) supports multiple remote service verification methods, such as Dynamic Host Configuration Protocol (DHCP) dialup emulation tests. This allows commissioning and configuration engineers to remotely verify services. In addition, this section describes how to verify the L2VPN service on site.

Copyright © Huawei Technologies Co., Ltd.

Prerequisites

- The OLT is properly connected to the upper-layer network.
- The DHCP server, Trivial File Transfer Protocol (TFTP) server, and softswitch or IP multimedia subsystem (IMS) have been configured.

Procedure

- Perform a DHCP dialup emulation test.

  In this test, a cable modem (CM) is emulated on the OLT to apply to the DHCP server for an IP address. This checks whether the OLT can communicate with the DHCP server and verifies CM DHCP configurations on the DHCP relay, proxy, and server.

  1. Run the **simulate dhcp start cm** *mac-address* [**option60** *option60*] command to start a DHCP dialup emulation test.

     NOTE

     You can run the **simulate dhcp stop** command to stop the DHCP emulation.

  2. Run the **display simulation dhcp** command to query the results of the DHCP dialup emulation test.
  3. Check whether the **User IP** has obtained an IP address.

- Check the CM status.

  Run the **display cable modem** command to query the CM status in **Status**.

```
huawei(config)#display cable modem  all

------------------------------------------------------------------------------
-
 Idx   MAC            IP              I/F          Status   Prim  Num Ver  DS
RX
                                                           SID   CPE
Power

------------------------------------------------------------------------------
-
 1     0023-ED6F-21A3 192.168.1.118   1/1/0/U4     ol-pt    1     0   D2.0
-

------------------------------------------------------------------------------
-
 Total:
1
 ol: 0, ol-ptd: 0, ol-pt: 1, ol-d: 0, wol: 0, wol-ptd: 0, wol-pt: 0, wol-d:
0,
pol: 0, pol-ptd: 0, pol-pt: 0, pol-d: 0, offline: 0, rej-m: 0, rej-pt: 0, rej-
o:
 0, init: 0, init-rc: 0, DHCP: 0, DHCP-O: 0, DHCP-R: 0, DHCP-C: 0, REG:
0
 Note: 1. Idx is the index of a
CM.
       2. The downstream received power is in the unit of
dBmV.
       3. In status, "ol" means online, "rej" means reject.
```

  The following table lists the CM status and handling suggestions.

Copyright © Huawei Technologies Co., Ltd.

CM Status	Description	Handling Suggestion
init	Indicates that the CM initialization ranging message is received.the CM initialization.	If a CM is always in the ranging state, the ranging fails. Then check radio frequency (RF) line indicators and detect line faults.
init-rc	Indicates that the CM initialization ranging is complete.	No action is required. The ranging of the CM is complete.
DHCP	Indicates that the DHCP discovery from the CM is received.	If a CM initiates a DHCP request but does not obtain an IP address, check the DHCP server, routing between the OLT and the DHCP server, and DHCP server parameter settings.
● DHCP-O ● DHCP-R ● DHCP-C	● DHCP-O: indicates that the offer from the DHCP server is received. ● DHCP-R: indicates that the DHCP request from the CM is received. ● DHCP-C: indicates that the acknowledge from the DHCP server is received.	The DHCP server has assigned an IP address to the CM and sent configuration file name and IP address of the TFTP or ToD server to the CM using the Option 67 and Option 66 fields (the Option 67 field carries the configuration file name and the Option 66 field carries the IP address of the TFTP or ToD server). If the CM is always in the DHCP-C state, the CM fails to obtain the configuration file. Then check the TFTP server, routing between the OLT and the TFTP server, and TFTP server parameter settings.
REG	Indicates that a registration is started.	If the CM is always in the register state, the CM obtains an incorrect configuration file. Then change the configuration file.

Copyright © Huawei Technologies Co., Ltd.

CM Status	Description	Handling Suggestion
● ol ● ol-pt ● ol-ptd ● ol-d ● wol ● wol-pt ● wol-ptd ● wol-d ● pol ● pol-pt ● pol-ptd	● ol: indicates that the CM is online. (valid only for CMs complying with DOCSIS 2.0) ● ol-pt: indicates that the CM is online and passes the BPI authentication. (valid only for CMs complying with DOCSIS 2.0) ● ol-ptd: indicates that the CM is online and passes the BPI authentication, and NetAccessEnable is disabled. (valid only for CMs complying with DOCSIS 2.0) ● ol-d: indicates that the CM is online and NetAccessEnable is disabled. (valid only for CMs complying with DOCSIS 2.0) ● wol: indicates that the CM is online and all channels bound to the CM are available. (valid only for CMs complying with DOCSIS 3.0) ● wol-pt: indicates that the CM is online and passes the BPI authentication, and all channels bound to the CM are available. (valid only for CMs complying with DOCSIS 3.0) ● wol-ptd: indicates that the CM is online and passes the BPI authentication, NetAccessEnable is disabled, and all channels bound to the CM are available. (valid only for CMs complying with DOCSIS 3.0) ● wol-d: indicates that the CM is online, NetAccessEnable is disabled, and all channels bound to the CM are available. (valid only for CMs complying with DOCSIS 3.0) ● pol: indicates that the CM is online and some channels	No action is required. The status indicates that the CM has registered

Copyright © Huawei Technologies Co., Ltd.

CM Status	Description	Handling Suggestion
● pol-d	bound to the CM are available. (valid only for CMs complying with DOCSIS 3.0) ● pol-pt: indicates that the CM is online and passes the BPI authentication, and some channels bound to the CM are available. (valid only for CMs complying with DOCSIS 3.0) ● pol-ptd: indicates that the CM is online and passes the BPI authentication, NetAccessEnable is disabled, and some channels bound to the CM are available. (valid only for CMs complying with DOCSIS 3.0) ● pol-d: indicates that the CM is online, NetAccessEnable is disabled, and some channels bound to the CM are available. (valid only for CMs complying with DOCSIS 3.0)	with the OLT and can correctly transmit and receive services.
offline	Indicates the offline status.	If the CM is in the offline state, check the power status, noise, and channel frequency of the CM.
● rej-m ● rej-pt ● rej-o	● rej-m: indicates that the MIC verification fails. ● rej-pt: indicates that the BPI authentication fails. ● rej-o: indicates that the authentication reject due to other reasons.	If the CM is in the reject state, no service flow can be created. Then check the CM authentication and CM message integrity check (MIC), and check whether class of service (COS) parameters specified in the CM configuration file are supported by the OLT.

- Verify that the L2VPN service can be provisioned.
  After the CM is installed in the enterprise and the switch connected to the CM is commissioned, L2VPN service can be provisioned.

----End

15.3.3 WLAN Hotspot Radio Backhaul Service Networking

In wireless local area network (WLAN) hotspot radio backhaul service networking, a distributed cable modem termination system (D-CMTS) connects to cable modems (CMs) through radio frequency (RF) ports. A CM connects to wireless access points (APs) to provide wireless fidelity

Copyright © Huawei Technologies Co., Ltd.

(Wi-Fi) access for users. This section describes how to configure the optical line terminal (OLT) to provision the WLAN hotspot radio backhaul service.

Service Requirements

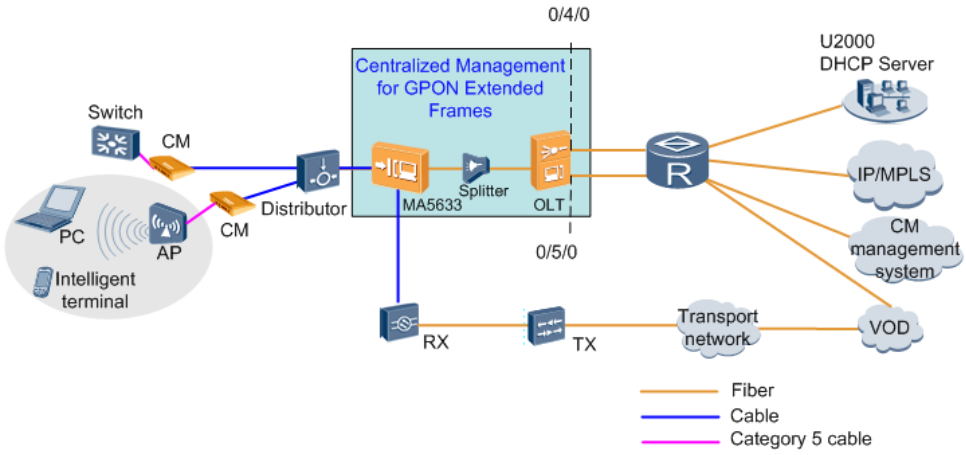
A network supplier needs to provide the Internet access service through Wi-Fi for a business area covered by APs.

Usage Scenario

As shown in **Figure 15-12**, a D-CMTS is deployed on an optical node and CMs are deployed at shops. The CMs connect to RF ports on the D-CMTS through cables.

- A CM connects to wireless APs to provide the WLAN hotspot radio backhaul service. The wireless APs provide Wi-Fi access for users.
- Wi-Fi users access the Internet through Dynamic Host Configuration Protocol (DHCP) dialup.
- The D-CMTS works as a GPON remote extended frame. This reduces D-CMTS management and maintenance costs and simplifies configurations.

Figure 15-12 WLAN hotspot radio backhaul service networking



Configuration

The method of configuring the WLAN hotspot radio backhaul service is the same as that of configuring the L2VPN enterprise service and therefore is not described in this section. For details, see **15.3.2.2 Configuration Process**.

15.4 Service Configuration on a D-CMTS That Works as a GE Remote Extended Frame on a Layer 3 Network

This section describes how to configure services, including the Internet access service, voice service, and VoD service, on an optical line terminal (OLT) when a distributed cable modem

Copyright © Huawei Technologies Co., Ltd.

termination system (D-CMTS) works as a GE remote extended frame on a Layer 3 network. The MA5603T equipped with the SCUV, ETHB, and SPUF boards is used as an example.

Control Board	SCUV
Cascading Board	ETHB: 0/3
SPU Board	SPUF: 0/4, 0/5

15.4.1 Home Service Networking

In home service networking, a distributed cable modem termination system (D-CMTS) connects to cable modems (CMs) at user homes through radio frequency (RF) ports and provides home services for users, including the cable TV (CATV) service, Internet access service, VoD service, broadband TV (BTV) service, and PacketCable service. This section describes how to configure the optical line terminal (OLT) to provision the home services.

NOTE

Configuration procedures are the same for IPv6 and IPv4 networks except in "Configure Dynamic Host Configuration Protocol (DHCP) relay" and "Configure a route". In addition, IPv6 does not support the function of configuring PacketCable dynamic voice services.

15.4.1.1 Service Requirements and Usage Scenario

Service Requirements

Users require the provisioning of the TV service, Internet access service, VoD service, broadband TV (BTV) service, and VoIP service. The TV service can be provisioned immediately after the distributed cable modem termination system (D-CMTS) hardware is connected. This section only describes how to configure the Internet access service, VoD service, BTV service, and VoIP service.

Usage Scenario

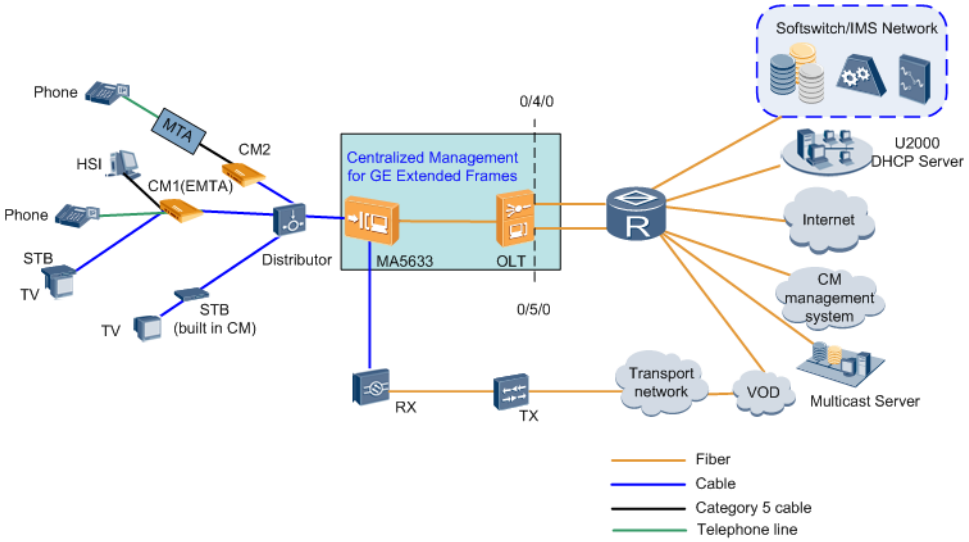
As shown in **Figure 15-13**, a distributed cable modem termination system (D-CMTS) is deployed on an optical node and cable modems (CMs) are deployed at user homes. The CMs connect to radio frequency (RF) ports on the MA5633 through cables.

- Port 1 on CM 1 connects to a PC for the Internet access service, port 2 connects to a phone set for the VoIP service, and the distributor connects to the STB for the VoD service. CM 1 supports embedded media terminal adapter (EMTA) functions and the voice users of CM 1 use PacketCable 1.x.
- CM 2 does not support EMTA functions and needs to connect to a media terminal adapter (MTA). The voice users of CM 2 use PacketCable Multimedia.
- Users access the Internet through Dynamic Host Configuration Protocol (DHCP) dialup.
- The IP addresses of the CM, STB, PC, and MTA are assigned by the DHCP server and in different network segments.

Copyright © Huawei Technologies Co., Ltd.

- The MA5633 works as a GE remote extended frame to reduce MA5633 management and maintenance costs and simplify configurations.

Figure 15-13 Home service networking

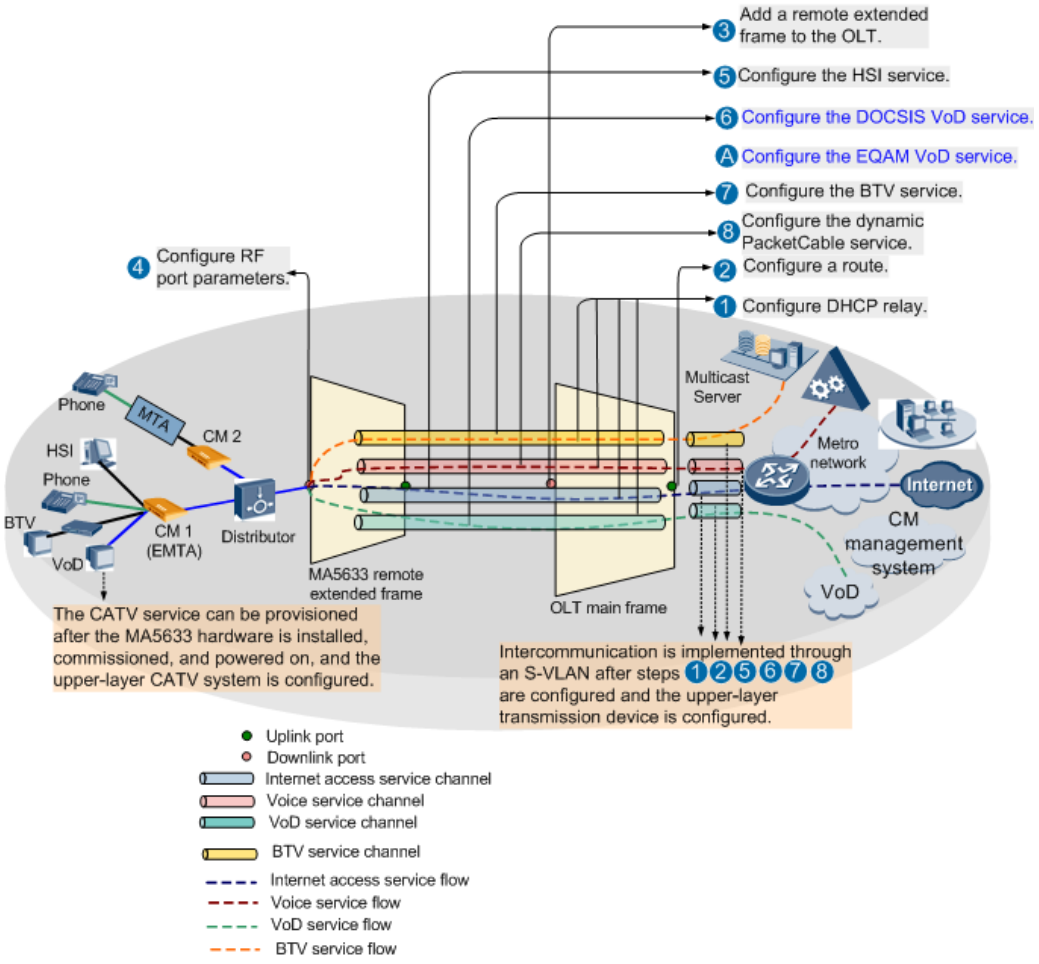


15.4.1.2 Configuration Process

Figure 15-14 shows the configuration roadmap for the home service networking.

Copyright © Huawei Technologies Co., Ltd.

Figure 15-14 Configuration roadmap for the home service networking



The following table describes the configuration steps. All configurations are issued from the optical line terminal (OLT).

No.	Step	Description
1	● IPv4: **Configure Dynamic Host Configuration Protocol (DHCP) relay.** ● IPv6: **Configure Dynamic Host Configuration Protocol (DHCP) relay (IPv6).**	This section describes how to configure Dynamic Host Configuration Protocol (DHCP) relay so that cable modems (CMs) can obtain IP addresses in different network segments.
2	● IPv4: **Configure a route.** ● IPv6: **Configure a route (IPv6).**	This section describes how to implement network communication by configuring a route in Layer 3 networking with an optical line terminal (OLT). Through the route, packets are forwarded at Layer 3 between the OLT and its upper-layer devices or servers.

Copyright © Huawei Technologies Co., Ltd.

No.	Step	Description
3	**Add a remote extended frame to the OLT.**	A distributed cable modem termination system (D-CMTS) that works as a GE remote extended frame connects to a port on a GE cascading board of an optical line terminal (OLT). You can configure the remote extended frame only after adding it to the OLT.
4	**Configure radio frequency (RF) port parameters.**	Radio frequency (RF) port parameters define the frequency spectrum range for signal transmission and modulation mode. The configuration of RF port parameters implements data service transmission over cables. RF port parameters can be configured using either of the following methods: ● Use a cable initialization profile to configure the parameters. ● Customize the parameters in cable mode.
5	**Configure the high-speed Internet (HSI) service.**	None
6	**Configure the VoD service.**	None
7	**Configure the broadband TV (BTV) service.**	None
8	**Configure the dynamic PacketCable service.**	None
9	**Verify the configured services.**	An OLT supports multiple remote service verification methods. This allows commissioning and configuration engineers to remotely verify services. 1. A DHCP dialup emulation test checks whether the OLT can communicate with the DHCP server and verifies CM DHCP configurations on the DHCP relay, proxy, and server. 2. The status of a CM can be queried. Based on the information, you can determine whether the CM is online.

15.4.1.3 Configuring DHCP Relay

This section describes how to configure Dynamic Host Configuration Protocol (DHCP) relay so that cable modems (CMs) can obtain IP addresses in different network segments.

Copyright © Huawei Technologies Co., Ltd.

Prerequisites

The upper-layer router, DHCP server, and Trivial File Transfer Protocol (TFTP) server of an optical line terminal (OLT) have been configured.

Data Plan

Table 15-29 DHCP data plan for the OLT

Item	Data
VLAN	ID of the CM management S-VLAN: 100; type of the VLAN: smart
DHCP server group parameters	● IP address of the DHCP domain gateway for CMs: 10.10.224.1; domain name: docsis ● IP address of the DHCP domain gateway for media terminal adapters (MTAs): 10.100.224.1; domain name: pktc ● IP address of the DHCP domain gateway for paid PCs: 10.100.187.1; domain name: default ● IP address of the DHCP domain gateway for overdue PCs: 10.100.8.1; domain name: default ● IP address of the DHCP domain gateway for set top boxes (STB): 10.200.160.1; domain name: stb

Table 15-30 Data plan for the upper-layer devices of the OLT

Item	IP Address
Layer 3 interfaces connecting the router to the OLT	● Forwarding DHCP and broadband packets: 11.11.11.11 ● Forwarding CM management, VoD, and multicast packets: 11.11.12.11
IP addresses of DHCP servers	● DHCP server assigning IP addresses to CMs and MTAs: 192.168.10.10-192.168.10.11 ● DHCP server assigning IP addresses to PCs and STBs: 192.168.10.12-192.168.10.13
IP address of the TFTP server	192.168.5.10-192.168.5.13

Procedure

Step 1 Set the IP addresses of Layer 3 VLAN interfaces.

```
huawei(config)#vlan 100 smart
huawei(config)#interface vlanif 100
huawei(config-if-vlanif100)#arp proxy enable
huawei(config-if-vlanif100)#ip address 10.10.224.1 255.255.255.0 description
```


Copyright © Huawei Technologies Co., Ltd.

```
docsis     //Set the IP address of the DHCP domain gateway for CMs.
huawei(config-if-vlanif100)#ip address 10.100.224.1 255.255.255.0 sub description
pktc     //Set the IP address of the DHCP domain gateway for MTAs.
huawei(config-if-vlanif100)#ip address 10.200.160.1 255.255.255.0 sub description
stb     //Set the IP address of the DHCP domain gateway for STBs.
huawei(config-if-vlanif100)#ip address 10.100.187.1 255.255.255.0 sub description
default     //Set the IP address of the DHCP domain gateway for paid PCs.
huawei(config-if-vlanif100)#ip address 10.100.8.1 255.255.255.0 sub description
default      //Set the IP address of the DHCP domain gateway for overdue PCs.
huawei(config-if-vlanif100)#quit
```

Step 2 Configure the working mode of the DHCP relay to Layer 3 Option 60.

In DHCP Option 60 mode, a DHCP server group is selected according to the Option 60 domain name in DHCP packets. Users in this mode are identified by domain information of packets, which differentiates various service types in a VLAN. Ensure that the Option 60 domain name and the DHCP server group bound to the Option 60 domain name are configured beforehand.

```
huawei(config)#dhcp mode layer-3 Option60
  Several minutes may be required and no action can be taken during this period
  Are you sure to perform this operation? (y/n)[n]: y
```

Step 3 Enable the DHCP option82 feature.

The DHCP feature does not have any mechanism for authentication or security. Thus, the DHCP feature encounters many security problems when it is used in the network. To solve these problems, the DHCP option82 is introduced.

```
huawei(config)#dhcp option82 enable
```

Step 4 Set the IP addresses of the servers in a DHCP server group.

```
huawei(config)#dhcp-server 0 ip 192.168.10.10 192.168.10.11    //Configure DHCP
server group 0 to assign IP addresses to CMs and MTAs.
huawei(config)#dhcp-server 1 ip 192.168.10.12 192.168.10.13    //Configure DHCP
server group 1 to assign IP addresses to PCs and STBs.
```

Step 5 Create a DHCP Option 60 domain.

```
huawei(config)#dhcp domain default   //Create Option 60 domain name default for
PCs.
huawei(config-dhcp-domain-default)#dhcp-gateway learning enable   //Paid and
overdue PCs are in different network segments. Therefore, self-learning needs to be
enabled on OLT gateways.
huawei(config-dhcp-domain-default)#dhcp-server 1 vlan 100       //Bind DHCP server
group 1 to the DHCP domain where the PCs locate. After the configuration, the PCs
in the DHCP domain are corresponded to DHCP server group 1.
huawei(config-dhcp-domain-default)#quit
huawei(config)#dhcp domain docsis   //Create Option 60 domain name docsis for CMs.
huawei(config-dhcp-domain-docsis)#dhcp-server 0 vlan 100       //Bind DHCP server
group 0 to the DHCP domain where the CMs locate. After the configuration, the CMs
in the DHCP domain are corresponded to DHCP server group 0.
huawei(config-dhcp-domain-docsis)#quit
huawei(config)#dhcp domain pktc   //Create Option 60 domain name pktc for MTAs.
huawei(config-dhcp-domain-pktc)#dhcp-server 0 vlan 100       //Bind DHCP server
group 0 to the DHCP domain where the MTAs locate. After the configuration, the CMs
in the DHCP domain are corresponded to DHCP server group 0.
huawei(config-dhcp-domain-pktc)#quit
huawei(config)#dhcp domain stb   //Create Option 60 domain name stb for STBs.
huawei(config-dhcp-domain-stb)#dhcp-server 1 vlan 100     //Bind DHCP server group
1 to the DHCP domain where the STBs locate. After the configuration, the STBs in
the DHCP domain are corresponded to DHCP server group 1.
huawei(config-dhcp-domain-stb)#quit
```

Step 6 Set IP addresses of the gateways for the DHCP domain.

```
huawei(config)#interface vlanif 100
huawei(config-if-vlanif100)#dhcp domain default gateway 10.100.187.1
```


Copyright © Huawei Technologies Co., Ltd.

```
10.100.8.1    //Set the IP address of the gateway for the PC domain to 10.100.187.1
for paid PCs and to 10.100.8.1 for overdue PCs.
huawei(config-if-vlanif100)#dhcp domain docsis gateway 10.10.224.1    //Set the IP
address of the gateway for the CM domain to 10.10.224.1.
huawei(config-if-vlanif100)#dhcp domain pktc gateway 10.100.224.1    //Set the IP
address of the gateway for the MTA domain to 10.100.224.1.
huawei(config-if-vlanif100)#dhcp domain stb gateway 10.200.160.1    //Set the IP
address of the gateway for the STB domain to 10.200.160.1.
huawei(config-if-vlanif100)#quit
```

----End

15.4.1.4 Configuring a Route

This section describes how to implement network communication by configuring a route in Layer 3 networking with an optical line terminal (OLT). Through the route, packets are forwarded at Layer 3 between the OLT and its upper-layer devices or servers.

Prerequisites

The upper-layer router has been configured.

Data Plan

Table 15-31 Data plan for the Layer 3 interfaces on the network side

Item	IP Address
Layer 3 interfaces on the OLT network side	Forwarding Dynamic Host Configuration Protocol (DHCP) and broadband packets: ● VLAN ID: 2004 ● Port number: 0/4/0 ● IP address: 11.11.11.10/24 Forwarding cable modem (CM) management, VoD, and multicast packets: ● VLAN ID: 2005 ● Port number: 0/5/0 ● IP address: 11.11.12.10/24
Layer 3 interfaces connecting the router to the OLT	● Forwarding DHCP and broadband packets: 11.11.11.11 ● Forwarding CM management, VoD, and multicast packets: 11.11.12.11

Copyright © Huawei Technologies Co., Ltd.

Item	IP Address
Upper-layer servers of the OLT	● DHCP servers: – DHCP server assigning IP addresses to CMs and media terminal adapters (MTAs): 192.168.10.10-192.168.10.11 – DHCP server assigning IP addresses to PCs and set top boxes (STBs): 192.168.10.12-192.168.10.13 ● CM management system, VoD server, and multicast server: 192.168.20.10-192.168.20.12 ● Softswitch or IP multimedia subsystem (IMS) server: 192.168.50.10

Procedure

Step 1 Create Layer 3 VLAN interfaces on the network side.

1. Create VLANs and configure their uplink ports.
   - VLAN 2004 is of the smart VLAN type and used for forwarding DHCP and broadband packets. Add uplink port 0/4/0 to VLAN 2004.
   - VLAN 2005 is of the smart VLAN type and used for forwarding CM management, VoD, and multicast packets. Add uplink port 0/5/0 to VLAN 2005.

```
huawei(config)#vlan 2004 to 2005 smart
huawei(config)#port vlan 2004 0/4 0
huawei(config)#port vlan 2005 0/5 0
```

2. (Optional) Create native VLANs for Ethernet outbound ports.

   Packets between the OLT and its upper-layer router are assumed to be forwarded at Layer 3 and no VLAN information is required. The created native VLANs remove VLAN tags from the packets transmitted out of Ethernet ports.

```
huawei(config)#interface eth 0/4
huawei(config-if-eth-0/4)#native-vlan 0 vlan 2004    //Remove VLAN tags from
the packets transmitted out of the 0/8/0 port.
huawei(config-if-eth-0/4)#quit
huawei(config)#interface eth 0/5
huawei(config-if-eth-0/5)#native-vlan 0 vlan 2005    //Remove VLAN tags from
the packets transmitted out of the 0/9/0 port.
huawei(config-if-eth-0/5)#quit
```

3. Create Layer 3 VLAN interfaces.
   a. Create a Layer 3 interface for VLAN 2004, through which DHCP and broadband packets are forwarded.

```
huawei(config)#interface vlanif 2004
huawei(config-if-vlanif2004)#ip address 11.11.11.10 255.255.255.0
huawei(config-if-vlanif2004)#quit
```

   b. Create a Layer 3 interface for VLAN 2005, through which CM management and VoD packets are forwarded.

```
huawei(config)#interface vlanif 2005
huawei(config-if-vlanif2005)#ip address 11.11.12.10 255.255.255.0
huawei(config-if-vlanif2005)#quit
```

Step 2 Configure static routes to implement the communication between the OLT and its upper-layer devices.

Copyright © Huawei Technologies Co., Ltd.

```
huawei(config)#ip route-static 0.0.0.0 0.0.0.0 11.11.11.11     //Broadband packets
are forwarded through the Layer 3 interface of VLAN 2004.
huawei(config)#ip route-static 192.168.20.0 255.255.255.0 11.11.12.11     //CM
management, VoD, and multicast packets are forwarded through the Layer 3 interface
of VLAN 2005.
huawei(config)#ip route-static 192.168.60.3 255.255.255.0 11.11.12.11     //COPS
packets are forwarded through the Layer 3 interface of VLAN 2005.
huawei(config)#ip route-static 192.168.10.0 255.255.255.0 11.11.11.11     //DHCP
packets are forwarded through the Layer 3 interface of VLAN 2004.
huawei(config)#ip route-static 192.168.5.0 255.255.255.0 11.11.12.11      //TFTP
server
huawei(config)#ip route-static 192.168.50.0 255.255.255.0 11.11.12.11     //
Softswitch or IMS server
```

NOTE

The interconnected router must set static routes and add the routes to dynamic routes.

----End

Result

The OLT can communicate with its upper-layer devices. To check network connectivity between two devices, run the **ping** and **tracert** commands.

The configured static routes can be queried in an IPv4 routing table by running the **display ip routing-table** command.

15.4.1.5 Configuring DHCP Relay (IPv6)

This section describes how to configure DHCPv6 relay so that terminals can obtain IP addresses in different network segments.

Prerequisites

The upper-layer router and DHCP server have been configured.

Data Plan

Table 15-32 DHCP data plan

Configuration Item	Data
Terminal-side of CM	● network segment of CM: 2001:0db8:0001::/64 ● network segment of PCs with fees paid: 2001:0db8:0003::/64 ● network segment of overdue PCs: 2001:0db8:0004::/64
User-side of OLT	● IP address of the gateway for the DHCP domain of CMs: 2001:0db8:0001::1/64; domain name: **docsis** ● IP address of the gateway for the DHCP domain of PCs with fees paid: 2001:0db8:0003::3/64; domain name: **default** ● IP address of the gateway for the DHCP domain of overdue PCs: 2001:0db8:0004::4/64; domain name: **default**

Copyright © Huawei Technologies Co., Ltd.

Configuration Item	Data
Network-side of OLT	Forwarding DHCP and broadband packets: ● VLAN ID: 2004 ● Port number: 0/4/0 ● IP address: 2001:0db8:0007::12/64 Forwarding CM management packets, multicast packets, and VoD packets: ● VLAN ID: 2005 ● Port number: 0/5/0 ● IP address: 2001:0db8:0008::13/64
Router	● IP address of the Layer 3 interface for forwarding DHCP and broadband packets: 2001:0db8:0007::6/64 ● IP address of the Layer 3 interface for forwarding CM management packets: 2001:0db8:0008::7/64
Server	● IP addresses of DHCP servers: – DHCP server allocating IP addresses for CMs: 2001:0db8:0006::8/64-2001:0db8:0006::9/64 – DHCP server allocating IP addresses for PCs: 2001:0db8:0006::10/64-2001:0db8:0006::11/64 ● IP addresses of the CM management system: 2001:0db8:0011::14/64-2001:0db8:0011::16/64

Procedure

Step 1 Configure a CM service provisioning mode, which can be IPv6 (preferentially used), APM, or DPM (used for dual-stack service provisioning). Select a mode based on site requirements.

```
huawei(config)#interface cable 1/1/0
huawei(config-if-cable-1/1/0)#cable ip-mode dpm
huawei(config-if-cable-1/1/0)#quit
```

Step 2 Configure the IP address of the VLAN Layer 3 interface.

```
huawei(config)#ipv6      //Enable IPv6 packet forwarding.
huawei(config)#vlan 100
huawei(config)#interface vlanif 100
huawei(config-if-vlanif100)#ipv6 enable     //Enable IPv6 on ports.
huawei(config-if-vlanif100)#undo ipv6 nd ra halt       //enables a router to send
RA messages.
huawei(config-if-vlanif100)#ipv6 nd autoconfig managed-address-flag    //Configure
the state-based auto-configuration address flag bit. The host obtains an IPv6
address using the state-based automatic configuration.
huawei(config-if-vlanif100)#ipv6 address 2001:0db8:0001::1/64     //Configure the
IP address of the gateway for the DHCP domain of CMs.
huawei(config-if-vlanif100)#ipv6 address 2001:0db8:0003::3/64     //Configure the
IP address of the gateway for the DHCP domain of PCs with fees paid.
huawei(config-if-vlanif100)#ipv6 address 2001:0db8:0004::4/64     //Configure the
IP address of the gateway for the DHCP domain of overdue PCs.
huawei(config-if-vlanif100)#quit
```


Copyright © Huawei Technologies Co., Ltd.

Step 3 Enable duplicate address detect (DAD) proxy, which prevents repeated link local addresses (LLAs) on the user side.

After receiving a DAD packet sent from the user side with destination IP address LLA, the OLT with DAD proxy enabled checks user online information based on the destination IP address and VLAN. If a user with the same IP address in the VLAN has been online, the OLT makes a response and prohibits the new user from going online. Otherwise, the OLT does not make a response.

```
huawei(config)#ipv6 dad proxy enable
huawei(config)#vlan service-profile profile-id 10
huawei(config)#vlan bind service-profile 100 profile-id 10
huawei(config-vlan-srvprof-10)#ipv6 dad proxy enable     //DAD proxy takes effect after it is enabled at system level and VLAN service profile level.
```

Step 4 Configure the working mode of DHCP relay to Layer 3 Option 16.

Option 16 is an option with code 16 in DHCPv6 packets, which identifies terminal types. In DHCPv6 Option 16 mode, packets select a DHCPv6 server based on the Option 16 domain. Therefore, in DHCPv6 Option 16 mode, packets select a DHCPv6 server based on terminal types.

```
huawei(config)#dhcpv6 mode layer-3 option16
  Several minutes may be required and no action can be taken during this period
  Are you sure to perform this operation? (y/n)[n]: y
```

Step 5 Enable DHCPv6 Option.

No authentication and security mechanisms are available for DHCPv6. Therefore, the application of DHCPv6 faces multiple security issues on networks. The enabled DHCPv6 Option function resolves these issues.

```
huawei(config)#dhcpv6 option enable
```

Step 6 Configure the IP addresses of the servers in a DHCP server group.

```
huawei(config)#dhcpv6-server 0 ipv6 2001:0db8:0006::8/64 2001:0db8:0006::9/64    //Configure DHCP server group 0 to allocate IP addresses for CMs.
huawei(config)#dhcpv6-server 1 ipv6 2001:0db8:0006::10/64 2001:0db8:0006::11/64    //Configure DHCP server group 1 to allocate IP addresses for PCs.
```

Step 7 Create DHCP Option 16 domains.

```
huawei(config)#dhcp domain default   //Create Option 16 domain default for PCs.
huawei(config-dhcp-domain-default)#dhcpv6-gateway learning enable   //PCs require different IP address segments based on fee payment state. Therefore, automatic gateway learning must be enabled on the OLT.
huawei(config-dhcp-domain-default)#dhcpv6-server 1 vlan 100        /Bind DHCP server group 1 to the DHCP domain of PCs. After the configuration, the PCs in this DHCP domain are mapped to DHCP server group 1.
huawei(config-dhcp-domain-default)#quit
huawei(config)#dhcp domain docsis   //Create Option 16 domain docsis for CMs.
huawei(config-dhcp-domain-docsis)#dhcpv6-server 0 vlan 100      //Bind DHCP server group 0 to the DHCP domain of CMs. After the configuration, the CMs in this DHCP domain are mapped to DHCP server group 0.
huawei(config-dhcp-domain-docsis)#quit
```

Step 8 Configure the IP addresses of the gateways for DHCP domains.

```
huawei(config)#interface vlanif 100
huawei(config-if-vlanif100)#dhcp domain default gateway ipv6 2001:0db8:0003::3/64 2001:0db8:0004::4/64    //Configure IP addresses of the gateways for the DHCP domain of PCs, including the IP address of the gateway for the PCs with fees paid and the IP address of the gateway for overdue PCs.
huawei(config-if-vlanif100)#dhcp domain docsis gateway ipv6 2001:0db8:0001::1/64    //Configure the IP address of the gateway for the DHCP
```


Copyright © Huawei Technologies Co., Ltd.

```
domain of CMs.

huawei(config-if-vlanif100)#quit
```

----End

15.4.1.6 Configuring a Route (IPv6)

This section describes how to implement network communication by configuring a route in Layer 3 networking with an OLT. Through the route, the OLT can forward packets at Layer 3 between the OLT and its upper-layer devices or servers.

Prerequisites

The upper-layer router of the OLT has been configured.

Data Plan

Table 15-33 DHCP data plan

Configuration Item	Data
Terminal-side of CM	● network segment of CM: 2001:0db8:0001::/64 ● network segment of PCs with fees paid: 2001:0db8:0003::/64 ● network segment of overdue PCs: 2001:0db8:0004::/64
User-side of OLT	● IP address of the gateway for the DHCP domain of CMs: 2001:0db8:0001::1/64; domain name: **docsis** ● IP address of the gateway for the DHCP domain of PCs with fees paid: 2001:0db8:0003::3/64; domain name: **default** ● IP address of the gateway for the DHCP domain of overdue PCs: 2001:0db8:0004::4/64; domain name: **default**
Network-side of OLT	Forwarding DHCP and broadband packets: ● VLAN ID: 2004 ● Port number: 0/4/0 ● IP address: 2001:0db8:0007::12/64 Forwarding CM management packets, multicast packets, and VoD packets: ● VLAN ID: 2005 ● Port number: 0/5/0 ● IP address: 2001:0db8:0008::13/64
Router	● IP address of the Layer 3 interface for forwarding DHCP and broadband packets: 2001:0db8:0007::6/64 ● IP address of the Layer 3 interface for forwarding CM management packets: 2001:0db8:0008::7/64

Copyright © Huawei Technologies Co., Ltd.

Configuration Item	Data
Server	● IP addresses of DHCP servers: – DHCP server allocating IP addresses for CMs: 2001:0db8:0006::8/64-2001:0db8:0006::9/64 – DHCP server allocating IP addresses for PCs: 2001:0db8:0006::10/64-2001:0db8:0006::11/64 ● IP addresses of the CM management system: 2001:0db8:0011::14/64-2001:0db8:0011::16/64

Procedure

Step 1 Create VLAN Layer 3 interfaces on the network side.

1. Create VLANs and add an uplink port to them, respectively.
   - VLAN 2004 used for forwarding DHCP and broadband packets is a smart VLAN. Add uplink port 0/4/0 to VLAN 2004.
   - VLAN 2005 used for forwarding CM management packets, multicast packets, and VoD packets is a smart VLAN. Add uplink port 0/5/0 to VLAN 2005.

   ```
   huawei(config)#vlan 2004 to 2005 smart
   huawei(config)#port vlan 2004 0/4 0
   huawei(config)#port vlan 2005 0/5 0
   ```

2. (Optional) Create native VLANs for Ethernet outbound ports.

   Packets between the OLT and its upper-layer router are forwarded at Layer 3 and no VLAN tag is required. The created native VLANs remove VLAN tags from the packets transmitted out of Ethernet ports.

   ```
   huawei(config)#interface eth 0/4
   huawei(config-if-eth-0/4)#native-vlan 0 vlan 2004    //The packets transmitted
   out of port 0/4/0 are untagged.
   huawei(config-if-eth-0/4)#quit
   huawei(config)#interface eth 0/5
   huawei(config-if-eth-0/5)#native-vlan 0 vlan 2005    //The packets transmitted
   out of port 0/5/0 are untagged.
   huawei(config-if-eth-0/5)#quit
   ```

3. Create VLAN Layer 3 interfaces.
   a. Create the Layer 3 interface of VLAN 2004, through which DHCP and broadband packets are forwarded.

      ```
      huawei(config)#interface vlanif 2004
      huawei(config-if-vlanif2004)#ipv6 address 2001:0db8:0007::12/64
      huawei(config-if-vlanif2004)#quit
      ```

   b. Create the Layer 3 interface of VLAN 2005, through which CM management packets, multicast packets, and VoD packets are forwarded.

      ```
      huawei(config)#interface vlanif 2005
      huawei(config-if-vlanif2005)#ipv6 address 2001:0db8:0008::13/64
      huawei(config-if-vlanif2005)#quit
      ```

Step 2 Configure static routes for the communication between the OLT and its upper-layer devices.

```
huawei(config)#ipv6 route-static ::/0 2001:0db8:0007::6/64     //Broadband packets
are forwarded through the Layer 3 interface of VLAN 2004.
huawei(config)#ipv6 route-static 2001:0db8:0011::/64 2001:0db8:0008::7/64     //CM
```


Copyright © Huawei Technologies Co., Ltd.

```
management packets are forwarded through the Layer 3 interface of VLAN 2005.
huawei(config)#ipv6 route-static 2001:0db8:0006::/64 2001:0db8:0007::6/64     //
DHCP packets are forwarded through the Layer 3 interface of VLAN 2004.
```

NOTE

Configure static routes on the router connected to the OLT. In addition, add the static routes to dynamic ones.

----End

Result

The OLT can communicate with its upper-layer devices. To check network connectivity between two devices, run the **ping ipv6** and **tracert ipv6** commands.

The configured static routes can be queried in an IPv6 routing table by running the **display ipv6 routing-table** command.

15.4.1.7 Adding a Remote Extended Frame to an OLT

A distributed cable modem termination system (D-CMTS) that works as a GE remote extended frame connects to a port on a GE cascading board of an optical line terminal (OLT). You can configure the remote extended frame only after adding it to the OLT.

Prerequisites

The D-CMTS management policy is set to **extend-frame**. To do so, run the **sysman centralized-mgmt primary** command.

Context

You can use either of the methods listed in the following table to add a remote extended frame to an OLT based on site requirements.

Table 15-34 Methods of adding a remote extended frame to an OLT

Method	Usage Scenario	Remarks
Add a remote extended frame in offline mode.	The remote extended frames must be deployed one by one. This method facilitates remote extended frame management.	The remote extended frame ID has been planned.
Add an automatically discovered remote extended frame.	A great number of remote extended frames need to be deployed. This method reduces manual configurations.	The remote extended frame ID does not need to be planned.

Copyright © Huawei Technologies Co., Ltd.

Data Plan

Table 15-35 Data plan

Item	Data
GE cascading board	Board: H801ETHB Port ID: 0/3/1 Remote extended frame ID: 1 **NOTE** The OLT uses the MA5603T as an example. The configuration method is the same for other OLTs. The only difference lies in slot IDs.

Procedure

- Add a remote extended frame in offline mode.

```
huawei(config)#interface eth 0/3
huawei(config-if-eth-0/3)#network-role extend
  This operation will reset the board. Are you sure to continue ? (y/n)[n]:y
huawei(config-if-eth-0/3)#quit
huawei(config)#frame add 1 MA5633 extending-port 0/3/1
```

- Add an automatically discovered remote extended frame.

  The OLT supports the adding of an automatically discovered GE remote extended frame. This function does not require manual confirmation, thereby simplifying the remote extended frame registration and adding flow.

```
huawei(config)#interface eth 0/3
huawei(config-if-eth-0/3)#network-role extend
  This operation will reset the board. Are you sure to continue ? (y/n)[n]:y
huawei(config-if-eth-0/3)#quit
```

----End

Result

The remote extended frame is online.

After adding the remote extended frame, run the **display frame info** command to query the remote extended frame status. Ensure that **Online state** is **online** and **State** is **normal**.

```
huawei(config)#display frame info 1
  ---------------------------------------------------------------------------
  Type:           MA5633
  State:          Normal
  Desc:           MA5633_1_extending_0/3/1
  Hardware:       MA5633
  Extend type:    ETH
  Extending port: 0 /3 /1   //The cascading port on the OLT is 0/3/1.
  Extended port:  1 /0 /0   //The ID of the remote extended frame is 1 and the uplink
port on the remote extended frame is 0/0/0.
  Online state:   Online
  MAC address:    60DE-447D-8711
  ---------------------------------------------------------------------------
```


Copyright © Huawei Technologies Co., Ltd.

Follow-up Procedure

If the remote extended frame cannot be discovered, follow the troubleshooting suggestions listed in the following table to rectify faults.

Possible Cause	Troubleshooting Suggestion
The D-CMTS works as a standalone NE and cannot work as a remote extended frame.	Replace the D-CMTS with the one that works as a remote extended frame.
The D-CMTS management policy is set to **stand-alone** on the OLT.	Run the **sysman centralized-mgmt primary** command to configure the D-CMTS management policy to **extend-frame**.
The number of remote extended frames on the OLT has reached the threshold.	Run the **frame delete** command to delete a remote extended frame that is no longer used from the OLT.
The working mode of the ports on the remote extended frame is not **extend**.	In Ethernet mode, run the **network-role extend** command to set the working mode of the ports to **extend**.

15.4.1.8 Configuring RF Port Parameters

Radio frequency (RF) port parameters define the frequency spectrum range for signal transmission and modulation mode. The configuration of RF port parameters implements data service transmission over cables.

Context

You can use either of the methods listed in the following table to configure RF port parameters based on site requirements.

Copyright © Huawei Technologies Co., Ltd.

Table 15-36 Methods of configuring RF port parameters

Method	Usage Scenario	Remarks
Use a cable initialization profile to configure RF port parameters.	A carrier needs to deploy remote extended frames in batches. This method reduces data configuration for remote extended frames, thereby improving service provisioning efficiency. Configure the RF parameter profile for the remote extended frames on the optical line terminal (OLT). After the remote extended frames are powered on and added to the OLT, the OLT automatically issues the RF parameter profile to the remote extended frames, without requiring any software configuration. **NOTE** After the cable initialization profile is configured, a remote extended frame uses the RF port parameters configured in the profile after going online, regardless of whether the remote extended frame in added in offline mode or automatically discovered by the OLT.	● If the RF port parameters are the same for all the remote extended frames to be deployed in batches, use the cable initialization profile to configure the parameters. ● If the RF port parameters are basically the same for all the remote extended frames to be deployed in batches, use the cable initialization profile to configure the parameters. Then modify parameter settings in customized cable configuration mode.
Customize RF port parameters in cable mode.	Requires differentiated plans and configurations for RF port parameters of remote extended frames and the remote extended frames must be configured one by one.	If the RF port parameters are greatly different for the remote extended frames to be deployed in batches, use this method to configure the parameters.

Data Plan

Table 15-37 Data plan for RF port parameters

Item	Data
RF port	1/1/0

Copyright © Huawei Technologies Co., Ltd.

Item	Data
Upstream channels	● IDs: 1-4 ● Type: European standard (default channel type) ● ID of the upstream channel modulation profile: 1 (by default) ● Channel central frequency (MHz): 29.8, 42.60, 49.00, and 55.4
Downstream channels	● IDs: 1-16 ● Type: European standard (default channel type) ● Channel central frequency (MHz): 602.00, 610.00, 618.00, ..., and 722.00

Procedure

- Use a cable initialization profile to configure RF port parameters.
  1. Configure the frequency spectrum range and channel type.

     In this example, the channel is of the European type. To change the type to North American, run the **cable** command.
  2. Configure RF port parameters for upstream channels and activate the upstream channels.

Parameter	Description
frequency and **channel-width**	A central frequency and a frequency bandwidth determine a frequency range, within which packets are transmitted. For example, the central frequency of a European channel is 55 MHz and the frequency bandwidth is 6400 kHz. Then the frequency range of the channel is 51.8-58.2 MHz.
modulation-profile	An upstream channel modulation profile defines parameters for processing the signals transmitted over the upstream channel. You do not need to configure an upstream channel modulation profile generally. Ports automatically bind to profile 1 by default.

The following configurations are used as an example to configure RF parameters for upstream channels:

- Number of upstream channels: 4
- Frequency bandwidth of the channels: 3.2 MHz (default value)

```
huawei(config)#interface cable init-template
huawei(config-cable-init-template)#cable upstream 1 frequency 29.8 enable
huawei(config-cable-init-template)#cable upstream 2 frequency 42.60
```


Copyright © Huawei Technologies Co., Ltd.

```
enable
huawei(config-cable-init-template)#cable upstream 3 frequency 49.00
enable
huawei(config-cable-init-template)#cable upstream 4 frequency 55.40
enable
```

3. Configure RF port parameters for downstream channels and activate the downstream channels.

Parameter	Description
modulation	A greater modulation mode value for downstream channels results in a higher channel bandwidth but weaker anti-interference capability. Therefore, configure the modulation mode based on site requirements. The default modulation mode is QAM256. This example uses the default setting.

The following configuration is used as an example to configure RF parameters for downstream channels: A total of 16 downstream channels have been purchased.

```
huawei(config-cable-init-template)#cable downstream 1 frequency 602.00
enable
huawei(config-cable-init-template)#cable downstream 2 frequency 610.00
enable
huawei(config-cable-init-template)#cable downstream 3 frequency 618.00
enable
huawei(config-cable-init-template)#cable downstream 4 frequency 626.00
enable
huawei(config-cable-init-template)#cable downstream 5 frequency 634.00
enable
huawei(config-cable-init-template)#cable downstream 6 frequency 642.00
enable
huawei(config-cable-init-template)#cable downstream 7 frequency 650.00
enable
huawei(config-cable-init-template)#cable downstream 8 frequency 658.00
enable
huawei(config-cable-init-template)#cable downstream 9 frequency 666.00
enable
huawei(config-cable-init-template)#cable downstream 10 frequency 674.00
enable
huawei(config-cable-init-template)#cable downstream 11 frequency 682.00
enable
huawei(config-cable-init-template)#cable downstream 12 frequency 690.00
enable
huawei(config-cable-init-template)#cable downstream 13 frequency 698.00
enable
huawei(config-cable-init-template)#cable downstream 14 frequency 706.00
enable
huawei(config-cable-init-template)#cable downstream 15 frequency 714.00
enable
huawei(config-cable-init-template)#cable downstream 16 frequency 722.00
enable
```

- Customize the RF port parameters in cable mode.

  NOTE

  The configuration is complete if you have configured the RF port parameters using a cable initialization profile. For details, see **Use a cable initialization profile to configure RF port parameters**. Perform this operation if you need to customize the RF port parameters of a remote extended frame.

Copyright © Huawei Technologies Co., Ltd.

1. Configure RF port parameters for upstream channels and activate the upstream channels.

```
huawei(config)#interface cable 1/1/0
huawei(config-if-cable-1/1/0)#cable upstream 1 frequency 29.8 enable
huawei(config-if-cable-1/1/0)#cable upstream 2 frequency 42.60 enable
huawei(config-if-cable-1/1/0)#cable upstream 3 frequency 49.00 enable
huawei(config-if-cable-1/1/0)#cable upstream 4 frequency 55.40 enable
```

2. Configure RF port parameters for downstream channels and activate the downstream channels.

```
huawei(config-if-cable-1/1/0)#cable downstream 1 frequency 602.00 enable
huawei(config-if-cable-1/1/0)#cable downstream 2 frequency 610.00 enable
huawei(config-if-cable-1/1/0)#cable downstream 3 frequency 618.00 enable
huawei(config-if-cable-1/1/0)#cable downstream 4 frequency 626.00 enable
huawei(config-if-cable-1/1/0)#cable downstream 5 frequency 634.00 enable
huawei(config-if-cable-1/1/0)#cable downstream 6 frequency 642.00 enable
huawei(config-if-cable-1/1/0)#cable downstream 7 frequency 650.00 enable
huawei(config-if-cable-1/1/0)#cable downstream 8 frequency 658.00 enable
huawei(config-if-cable-1/1/0)#cable downstream 9 frequency 666.00 enable
huawei(config-if-cable-1/1/0)#cable downstream 10 frequency 674.00 enable
huawei(config-if-cable-1/1/0)#cable downstream 11 frequency 682.00 enable
huawei(config-if-cable-1/1/0)#cable downstream 12 frequency 690.00 enable
huawei(config-if-cable-1/1/0)#cable downstream 13 frequency 698.00 enable
huawei(config-if-cable-1/1/0)#cable downstream 14 frequency 706.00 enable
huawei(config-if-cable-1/1/0)#cable downstream 15 frequency 714.00 enable
huawei(config-if-cable-1/1/0)#cable downstream 16 frequency 722.00 enable
```

----End

Result

1. The transmit power of the downstream channels meets site requirements.

   Run the **display cable downstream** *frameid/slotid/portid* { **all** | *channel-id* } **status** command to check whether the RF port parameters meet site requirements.

2. The signal-to-noise (SNR) ratio of the upstream channels meets site requirements.

   Run the **display cable signal quality** [*frameid/slotid/portid* [**upstream** *channel-id*]] command to check whether the RF port parameters meet site requirements. A greater SNR ratio results in better signal quality. The recommended SNR ratio is greater than 30 dB.

15.4.1.9 Configuring the HSI Service

A cable modem (CM) connects to a distributed cable modem termination system (D-CMTS) through a cable and provides the high-speed Internet (HSI) service for users.

Data Plan

Table 15-38 Data plan for the HSI service

Item	Data
VLAN	ID of the HSI service VLAN (S-VLAN): 100; type of the VLAN: smart

Copyright © Huawei Technologies Co., Ltd.

Item	Data
Uplink ports	Forwarding Dynamic Host Configuration Protocol (DHCP), broadband, and VoIP packets: 0/4/0 Forwarding cable modem (CM) management and VoD packets: 0/5/0

Procedure

Step 1 Create an S-VLAN.

The S-VLAN is a user-side service VLAN between the optical line terminal (OLT) and the D-CMTS. The OLT works in Layer 3 forwarding mode.

```
huawei(config)#vlan 100 smart
```

Step 2 Create a CM S-VLAN.

The CM S-VLAN identifies a CM service flow. After the CM S-VLAN is configured, the OLT automatically creates a CM service flow when the CM goes online.

NOTE

- The **cable service-vlan** *vlanid* command is used to configure a global S-VLAN for CM services. After the configuration, all CM services of the D-CMTSs connected to the same OLT use the same VLAN. When the number of IP address segments planned for an OLT is less than eight, this command is recommended.
- The **cable service-vlan** *vlanid frameid/slotid* command is used to configure an S-VLAN for CM services on a specified D-CMTS. After the configuration, the D-CMTS does not use the global S-VLAN. When the number of IP address segments planned for an OLT is greater than eight, this command is recommended.

```
huawei(config)#cable service-vlan 100
  Info: The new service VLAN will take effect after the CM is restarted, are you
 sure to modify? (y/n)[n]:y
```

----End

15.4.1.10 Configuring the DOCSIS VoD Service

A cable modem (CM) connects to a distributed cable modem termination system (D-CMTS) through a cable and provides the DOCSIS VoD service for users.

Context

All home services use a service VLAN (S-VLAN) and the S-VLAN is globally configured. If the S-VLAN has been configured for other home services, use the S-VLAN for the VoD service.

Data Plan

Table 15-39 Data plan for the VoD service

Item	Data
VLAN	ID of the VoD S-VLAN: 100; type of the VLAN: smart

Copyright © Huawei Technologies Co., Ltd.

Item	Data
Uplink ports	Forwarding Dynamic Host Configuration Protocol (DHCP), broadband, and VoIP packets: 0/4/0 Forwarding cable modem (CM) management, VoD, and multicast packets: 0/5/0

Procedure

Step 1 Create an S-VLAN.

The S-VLAN is a user-side service VLAN between the optical line terminal (OLT) and the D-CMTS. The OLT works in Layer 3 forwarding mode.

```
huawei(config)#vlan 100 smart
```

Step 2 Create a CM S-VLAN.

The CM S-VLAN identifies a CM service flow. After the CM S-VLAN is configured, the OLT automatically creates a CM service flow when the CM goes online.

NOTE

- The **cable service-vlan** *vlanid* command is used to configure a global S-VLAN for CM services. After the configuration, all CM services of the D-CMTSs connected to the same OLT use the same VLAN. When the number of IP address segments planned for an OLT is less than eight, this command is recommended.
- The **cable service-vlan** *vlanid frameid/slotid* command is used to configure an S-VLAN for CM services on a specified D-CMTS. After the configuration, the D-CMTS does not use the global S-VLAN. When the number of IP address segments planned for an OLT is greater than eight, this command is recommended.

```
huawei(config)#cable service-vlan 100
  Info: The new service VLAN will take effect after the CM is restarted, are you
 sure to modify? (y/n)[n]:y
```

----End

15.4.1.11 Configuring the EQAM VoD Service

If the MA5633 is equipped with a built-in EQAM module, the MA5633 sets idle downstream DOCSIS channels as EQAM channels to transmit VoD data.

Prerequisites

The MA5633 supports built-in EQAM.

Context

In multiservice operator (MSO)-oriented solutions, both HFC networks and STBs use the broadcast television QAM technology and support only RF signals.

Video data is encapsulated into IP and UDP packet headers that are transmitted on IP networks, which cannot be transmitted on HFC networks. To transmit the video data on HFC networks, the video data must be modulated into RF signals using the EQAM module.

Copyright © Huawei Technologies Co., Ltd.

Video data transmission on HFC networks uses existing CATV coaxial cables on the HFC networks, thereby reducing network deployment costs.

Data Plan

Table 15-40 Data plan for the VoD service

Item	Data
EQAM IP address	10.10.10.10
VLAN	ID of the VoD S-VLAN: 50; type of the VLAN: smart
Uplink port	Forwarding CM management, VoD, and multicast packets: 0/5/0
EQAM channel ID	13-16
Modulation mode	QAM 64
Symbol rate	6.875
UDP port number	501-514

Procedure

Step 1 Use a cable initialization profile to configure RF port parameters.

```
huawei(config)#interface cable init-template
huawei(config-cable-init-template)#cable downstream 13 frequency 115.0 modulation
qam64 enable channel-mode eqam symbol-rate 6.875
huawei(config-cable-init-template)#cable downstream 14 frequency 123.00 modulation
qam64 enable channel-mode eqam symbol-rate 6.875
huawei(config-cable-init-template)#cable downstream 15 frequency 131.00 modulation
qam64 enable channel-mode eqam symbol-rate 6.875
huawei(config-cable-init-template)#cable downstream 16 frequency 139.00 modulation
qam64 enable channel-mode eqam symbol-rate 6.875
huawei(config-cable-init-template)#quit
```

Step 2 Configure a video profile.

A video profile contains all video mappings on an EQAM module and supports batch video mapping configurations. This facilitates video mapping configuration and management.

```
huawei(config)#cable eqam video profile name vod1
huawei(config-eqam-video-profile-vod1)#mapping index 1 type spts udp-port 501
output-program 1 pmtpid 32 channel 13
huawei(config-eqam-video-profile-vod1)#mapping index 2 type spts udp-port 502
output-program 2 pmtpid 48 channel 13
huawei(config-eqam-video-profile-vod1)#mapping index 3 type spts udp-port 503
output-program 3 pmtpid 64 channel 13
huawei(config-eqam-video-profile-vod1)#mapping index 4 type spts udp-port 504
output-program 4 pmtpid 80 channel 13
huawei(config-eqam-video-profile-vod1)#mapping index 5 type spts udp-port 505
output-program 1 pmtpid 96 channel 14
huawei(config-eqam-video-profile-vod1)#mapping index 6 type spts udp-port 506
output-program 2 pmtpid 112 channel 14
huawei(config-eqam-video-profile-vod1)#mapping index 7 type spts udp-port 507
output-program 3 pmtpid 128 channel 14
huawei(config-eqam-video-profile-vod1)#mapping index 8 type spts udp-port 508
output-program 1 pmtpid 160 channel 15
```


Copyright © Huawei Technologies Co., Ltd.

```
huawei(config-eqam-video-profile-vod1)#mapping index 9 type spts udp-port 509
output-program 2 pmtpid 176 channel 15
huawei(config-eqam-video-profile-vod1)#mapping index 10 type spts udp-port 510
output-program 1 pmtpid 224 channel 16
huawei(config-eqam-video-profile-vod1)#mapping index 11 type spts udp-port 511
output-program 2 pmtpid 240 channel 16
huawei(config-eqam-video-profile-vod1)#mapping index 12 type spts udp-port 512
output-program 3 pmtpid 256 channel 16
huawei(config-eqam-video-profile-vod1)#mapping index 13 type spts udp-port 513
output-program 4 pmtpid 272 channel 16
huawei(config-eqam-video-profile-vod1)#mapping index 14 type spts udp-port 514
output-program 5 pmtpid 288 channel 16
huawei(config-eqam-video-profile-vod1)#quit
```

NOTE

To configure video mappings in batches, do as follows:

```
huawei(config)#cable eqam video profile name vod1
huawei(config-eqam-video-profile-vod1)#mapping index 1 type spTS udp-port 501
output-program 1 pmtpid 32 chan
nel 13 number 4 increment output-program 1 pmtpid 32 udp-port 1
huawei(config-eqam-video-profile-vod1)#mapping index 5 type spts udp-port 505
output-program 1 pmtpid 96 chan
nel 14 number 3 increment output-program 1 pmtpid 32 udp-port 1
huawei(config-eqam-video-profile-vod1)#mapping index 8 type spts udp-port 508
output-program 1 pmtpid 160 chan
nel 15 number 2 increment output-program 1 pmtpid 32 udp-port 1
huawei(config-eqam-video-profile-vod1)#mapping index 10 type spts udp-port 510
output-program 1 pmtpid 224 chan
nel 16 number 5 increment output-program 1 pmtpid 32 udp-port 1
```

Step 3 Configure the VoD S-VLAN.

VLAN 50 is the S-VLAN that functions between the OLT and the MA5633. The OLT works in Layer 3 forwarding mode.

```
huawei(config)#vlan 50 smart
huawei(config)#port vlan 50 0/5 0
```

Step 4 Configure a video domain.

A video domain defines the relationships between an EQAM module and an EQAM IP address, and between the S-VLAN used for video data forwarding on an EQAM module, the EQAM module, and a video profile. This facilitates data management.

```
huawei(config)#cable eqam video domain huawei
huawei(config-eqam-domain-huawei)#local ip 10.10.10.10 vlan 50
huawei(config-eqam-domain-huawei)#bind video profile name vod1 1/1/0
huawei(config-eqam-domain-huawei)#quit
```

----End

Result

The MA5633 supports packet statistics query. Based on the statistical results, you can determine whether users can order programs and whether packet loss occurs in program transmitting.

- Run the **display cable eqam video stream** command to check the TS status. If the status is **online**, the TS is functional.
- Run the **display cable eqam video statistics input** command to query packet statistics and network jitter of a TS on the video service input end.

  Check whether the program ordered by a user has been sent to the MA5633. If the program has been sent to the MA5633, check whether the program traffic is normal.

Copyright © Huawei Technologies Co., Ltd.

- Run the **display cable eqam video statistics output** command to query packet statistics of a TS on the video service output end.

  Check whether the TS contains the ordered program, whether the program has been sent to the STB, and whether the TS traffic is normal.

15.4.1.12 Configuring the BTV Service

A cable modem (CM) connects to a distributed cable modem termination system (D-CMTS) through a cable and provides the multicast service for users.

Context

All home services use a service VLAN (S-VLAN) and the S-VLAN is globally configured. If the S-VLAN has been configured for other home services, use the S-VLAN for the multicast service.

Data Plan

Table 15-41 Data plan for the multicast service

Item	Data
VLAN	ID of the multicast S-VLAN: 100; type of the VLAN: smart
Uplink ports	Forwarding Dynamic Host Configuration Protocol (DHCP), broadband, and VoIP packets: 0/4/0 Forwarding cable modem (CM) management, VoD, and multicast packets: 0/5/0

Procedure

Step 1 Create an S-VLAN.

The S-VLAN is a user-side service VLAN between the optical line terminal (OLT) and the D-CMTS. The OLT works in Layer 3 forwarding mode.

```
huawei(config)#vlan 100 smart
```

Step 2 Create a CM S-VLAN.

The CM S-VLAN identifies a CM service flow. After the CM S-VLAN is configured, the OLT automatically creates a CM service flow when the CM goes online.

NOTE

- The **cable service-vlan** *vlanid* command is used to configure a global S-VLAN for CM services. After the configuration, all CM services of the D-CMTSs connected to the same OLT use the same VLAN. When the number of IP address segments planned for an OLT is less than eight, this command is recommended.
- The **cable service-vlan** *vlanid frameid/slotid* command is used to configure an S-VLAN for CM services on a specified D-CMTS. After the configuration, the D-CMTS does not use the global S-VLAN. When the number of IP address segments planned for an OLT is greater than eight, this command is recommended.

Copyright © Huawei Technologies Co., Ltd.

```
huawei(config)#cable service-vlan 100
  Info: The new service VLAN will take effect after the CM is restarted, are you
 sure to modify? (y/n)[n]:y
```

Step 3 Configure multicast VLAN 100.

NOTE

This configuration takes effect only after the CMs go online again.

```
huawei(config)#multicast-vlan 100
```

Step 4 Configure the Internet Group Management Protocol (IGMP) version to IGMPv3.

```
huawei(config-mvlan100)#igmp version v3
```

Step 5 Configure a multicast program generation mode.

Multicast programs can be dynamically or statically generated. For the D-CMTS, the multicast programs are dynamically generated.

```
huawei(config-mvlan100)#igmp mode off
  Are you sure to close IGMP? (y/n)[n]:y
huawei(config-mvlan100)#igmp match mode disable
```

Step 6 Configure the multicast uplink port to 0/5/0.

```
huawei(config-mvlan100)#igmp uplink-port 0/5/0
```

Step 7 Configure the IGMP mode to IGMP proxy.

```
huawei(config-mvlan100)#igmp mode proxy
  Are you sure to change IGMP mode?(y/n)[n]:y
huawei(config-mvlan100)#quit
```

Step 8 Bind CM multicast users to the multicast VLAN.

NOTE

This configuration takes effect only after the CMs go online again.

```
huawei(config)#cable multicast-vlan 100
```

Step 9 (Optional) Disable multicast DSID-based forwarding (MDF).

Multicast DSID-based forwarding is defined in data over cable service interface specification (DOCSIS) 3.0, perform this step if the CMs comply with DOCSIS 2.0.

Disable MDF if the CMTS is connected to a CM equipped with a TI chip. Otherse, the CM may go online and offline repeatedly.

```
huawei(config)#cable multicast mdf disable
```

Step 10 (Optional) Configure multicast user authentication.

NOTE

Perform this step if the configuration file on the CM server contains only the multicast rights profile name and the multicast rights must be configured on the D-CMTS.

The following configurations are used as an example to configure multicast user authentication:

- Multicast authentication function: enabled globally
- Maximum number of programs can be ordered if the CM does not match any rights rule: 32
- IP addresses of the multicast programs that can be ordered by multicast users: 225.1.1.1 and 225.1.1.2
- IP address of the multicast server: 192.168.20.11

Copyright © Huawei Technologies Co., Ltd.

- Multicast program priorities: 254 and 255

```
huawei(config)#cable multicast authorization enable max-sessions 32 default-acti
on permit
huawei(config)#cable multicast auth-profile profile-name btv1
huawei(config-multicast-profile-btv1)#rule 1 priority 255 group-ip 225.1.1.1 gro
up-ip-mask 24 src-ip 192.168.20.11 src-ip-mask 24 permit
huawei(config-multicast-profile-btv1)#rule 1 priority 254 group-ip 225.1.1.2 gro
up-ip-mask 24 src-ip 192.168.20.11 src-ip-mask 24 permit
```

Step 11 (Optional) Configure cable multicast version.

```
huawei(config)#cable multicast igmp-version v3
```

----End

15.4.1.13 Configuring the Dynamic PacketCable Service

A cable modem (CM) connects to a distributed cable modem termination system (D-CMTS) through a cable and provides the dynamic PacketCable service for users.

Context

Table 15-42 Data plan for the PacketCable service on the OLT

Item	Data
Uplink port	Forwarding VoIP packets: 0/4/0
VLAN	ID of service VLAN: 100 ID of the common open policy service (COPS) connection VLAN: 1000
IP address for creating a COPS connection to an IP multimedia subsystem (IMS) or a softswitch	192.168.60.3/24 (in the same network segment as the IMS or softswitch or can communicate with the IMS or softswitch)

Procedure

Step 1 Create a service VLAN (S-VLAN).

NOTE

All home services use an S-VLAN and the S-VLAN is globally configured. If the S-VLAN has been configured for other home services, use the S-VLAN in steps **Step 1** and **Step 2**.

The ID of S-VLAN is 100 and the type of the VLAN is smart. The S-VLAN is a user-side service VLAN between the OLT and the D-CMTS. The OLT works in Layer 3 forwarding mode.

```
huawei(config)#vlan 100 smart
```

Step 2 Create a CM S-VLAN.

The CM S-VLAN identifies a CM service flow. After the CM S-VLAN is configured, the OLT automatically creates a CM service flow when the CM goes online.

Copyright © Huawei Technologies Co., Ltd.

NOTE

- The **cable service-vlan** *vlanid* command is used to configure a global S-VLAN for CM services. After the configuration, all CM services of the D-CMTSs connected to the same OLT use the same VLAN. When the number of IP address segments planned for an OLT is less than eight, this command is recommended.
- The **cable service-vlan** *vlanid frameid/slotid* command is used to configure an S-VLAN for CM services on a specified D-CMTS. After the configuration, the D-CMTS does not use the global S-VLAN. When the number of IP address segments planned for an OLT is greater than eight, this command is recommended.

```
huawei(config)#cable service-vlan 100
  Info: The new service VLAN will take effect after the CM is restarted, are you
 sure to modify? (y/n)[n]:y
```

Step 3 Configure the Layer 3 interface for COPS connections.

```
huawei(config)#vlan 1000 smart
huawei(config)#interface vlanif 1000
huawei(config-if-vlanif1000)#ip address 192.168.60.3 24
huawei(config-if-vlanif1000)#quit
huawei(config)#port vlan 1000 0/4 0
```

Step 4 Configure a COPS connection.

The following configurations are used as an example to configure a COPS connection:

- COPS policy enforcement point (PEP) ID: IP address of the Layer 3 interface for the COPS connection
- Transmit and receive buffer for TCP sockets: 12 KB
- Differentiated services code point (DSCP) priority of COPS packets: ef

```
huawei(config)#cops pepid 192.168.60.3
huawei(config)#cops tcp window 12
huawei(config)#cops ip dscp ef
```

Step 5 Configure PacketCable parameters.

PacketCable 1.x parameter settings are as follows:

- Embedded media terminal adapter (EMTA) creating a dynamic media stream: permitted
- Other parameters: default settings

```
huawei(config)#packetcable 1dotx enable
huawei(config)#packetcable authorize common-docsis-mta enable
huawei(config)#packetcable multimedia enable
```

----End

15.4.1.14 Verifying Services

A distributed cable modem termination system (D-CMTS) working as a remote extended frame locates on an optical node. To facilitate service verification, the optical line terminal (OLT) supports multiple remote service verification methods, such as Dynamic Host Configuration Protocol (DHCP) dialup emulation tests. This allows commissioning and configuration engineers to remotely verify services. In addition, this section describes how to verify the home services on site.

Prerequisites

- The OLT is properly connected to the upper-layer network.

Copyright © Huawei Technologies Co., Ltd.

- The DHCP server, Trivial File Transfer Protocol (TFTP) server, and softswitch or IP multimedia subsystem (IMS) have been configured.

Procedure

- Perform a DHCP dialup emulation test.

  In this test, a cable modem (CM) is emulated on the OLT to apply to the DHCP server for an IP address. This checks whether the OLT can communicate with the DHCP server and verifies CM DHCP configurations on the DHCP relay, proxy, and server.

  1. Run the **simulate dhcp start cm** *mac-address* [**option60** *option60*] command to start a DHCP dialup emulation test.

     NOTE

     You can run the **simulate dhcp stop** command to stop the DHCP emulation.
  2. Run the **display simulation dhcp** command to query the results of the DHCP dialup emulation test.
  3. Check whether the **User IP** has obtained an IP address.
- Check the CM status.

  Run the **display cable modem** command to query the CM status in **Status**.

```
huawei(config)#display cable modem  all

------------------------------------------------------------------------------
-
 Idx   MAC            IP              I/F          Status   Prim  Num Ver  DS
RX
                                                            SID   CPE
Power

------------------------------------------------------------------------------
-
 1     0023-ED6F-21A3 192.168.1.118   1/1/0/U4     ol-pt    1     0   D2.0
-

------------------------------------------------------------------------------
-
 Total:
1
 ol: 0, ol-ptd: 0, ol-pt: 1, ol-d: 0, wol: 0, wol-ptd: 0, wol-pt: 0, wol-d:
0,
pol: 0, pol-ptd: 0, pol-pt: 0, pol-d: 0, offline: 0, rej-m: 0, rej-pt: 0, rej-
o:
 0, init: 0, init-rc: 0, DHCP: 0, DHCP-O: 0, DHCP-R: 0, DHCP-C: 0, REG:
0
 Note: 1. Idx is the index of a
CM.
       2. The downstream received power is in the unit of
dBmV.
       3. In status, "ol" means online, "rej" means reject.
```

  The following table lists the CM status and handling suggestions.

Copyright © Huawei Technologies Co., Ltd.

CM Status	Description	Handling Suggestion
init	Indicates that the CM initialization ranging message is received.the CM initialization.	If a CM is always in the ranging state, the ranging fails. Then check radio frequency (RF) line indicators and detect line faults.
init-rc	Indicates that the CM initialization ranging is complete.	No action is required. The ranging of the CM is complete.
DHCP	Indicates that the DHCP discovery from the CM is received.	If a CM initiates a DHCP request but does not obtain an IP address, check the DHCP server, routing between the OLT and the DHCP server, and DHCP server parameter settings.
● DHCP-O ● DHCP-R ● DHCP-C	● DHCP-O: indicates that the offer from the DHCP server is received. ● DHCP-R: indicates that the DHCP request from the CM is received. ● DHCP-C: indicates that the acknowledge from the DHCP server is received.	The DHCP server has assigned an IP address to the CM and sent configuration file name and IP address of the TFTP or ToD server to the CM using the Option 67 and Option 66 fields (the Option 67 field carries the configuration file name and the Option 66 field carries the IP address of the TFTP or ToD server). If the CM is always in the DHCP-C state, the CM fails to obtain the configuration file. Then check the TFTP server, routing between the OLT and the TFTP server, and TFTP server parameter settings.
REG	Indicates that a registration is started.	If the CM is always in the register state, the CM obtains an incorrect configuration file. Then change the configuration file.

Copyright © Huawei Technologies Co., Ltd.

CM Status	Description	Handling Suggestion
● ol ● ol-pt ● ol-ptd ● ol-d ● wol ● wol-pt ● wol-ptd ● wol-d ● pol ● pol-pt ● pol-ptd	● ol: indicates that the CM is online. (valid only for CMs complying with DOCSIS 2.0) ● ol-pt: indicates that the CM is online and passes the BPI authentication. (valid only for CMs complying with DOCSIS 2.0) ● ol-ptd: indicates that the CM is online and passes the BPI authentication, and NetAccessEnable is disabled. (valid only for CMs complying with DOCSIS 2.0) ● ol-d: indicates that the CM is online and NetAccessEnable is disabled. (valid only for CMs complying with DOCSIS 2.0) ● wol: indicates that the CM is online and all channels bound to the CM are available. (valid only for CMs complying with DOCSIS 3.0) ● wol-pt: indicates that the CM is online and passes the BPI authentication, and all channels bound to the CM are available. (valid only for CMs complying with DOCSIS 3.0) ● wol-ptd: indicates that the CM is online and passes the BPI authentication, NetAccessEnable is disabled, and all channels bound to the CM are available. (valid only for CMs complying with DOCSIS 3.0) ● wol-d: indicates that the CM is online, NetAccessEnable is disabled, and all channels bound to the CM are available. (valid only for CMs complying with DOCSIS 3.0) ● pol: indicates that the CM is online and some channels	No action is required. The status indicates that the CM has registered

Copyright © Huawei Technologies Co., Ltd.

CM Status	Description	Handling Suggestion
● pol-d	bound to the CM are available. (valid only for CMs complying with DOCSIS 3.0) ● pol-pt: indicates that the CM is online and passes the BPI authentication, and some channels bound to the CM are available. (valid only for CMs complying with DOCSIS 3.0) ● pol-ptd: indicates that the CM is online and passes the BPI authentication, NetAccessEnable is disabled, and some channels bound to the CM are available. (valid only for CMs complying with DOCSIS 3.0) ● pol-d: indicates that the CM is online, NetAccessEnable is disabled, and some channels bound to the CM are available. (valid only for CMs complying with DOCSIS 3.0)	with the OLT and can correctly transmit and receive services.
offline	Indicates the offline status.	If the CM is in the offline state, check the power status, noise, and channel frequency of the CM.
● rej-m ● rej-pt ● rej-o	● rej-m: indicates that the MIC verification fails. ● rej-pt: indicates that the BPI authentication fails. ● rej-o: indicates that the authentication reject due to other reasons.	If the CM is in the reject state, no service flow can be created. Then check the CM authentication and CM message integrity check (MIC), and check whether class of service (COS) parameters specified in the CM configuration file are supported by the OLT.

- Verify that home services can be provisioned.
  1. After the CM is installed at a user home and commissioned, the user can watch TV programs.
  2. After the high-speed Internet (HSI) service is provisioned, the user can access the Internet from a PC.
  3. After the VoD service is provisioned, the user can order programs.
  4. After the VoIP service is provisioned, the user can make and receive phone calls.

Copyright © Huawei Technologies Co., Ltd.

5. After the multicast service is provisioned, the user can watch ordered multicast programs.

----End

15.4.2 L2VPN Enterprise Service Networking

In L2VPN enterprise service networking, a distributed cable modem termination system (D-CMTS) connects to cable modems (CMs) through radio frequency (RF) ports, and the CMs connect to switches or routers to provide the L2VPN service for users. This section describes how to configure the optical line terminal (OLT) to provision the L2VPN service.

NOTE

Configuration procedures are the same for IPv6 and IPv4 networks except in "Configure Dynamic Host Configuration Protocol (DHCP) relay" and "Configure a route".

15.4.2.1 Service Requirements and Usage Scenario

Service Requirements

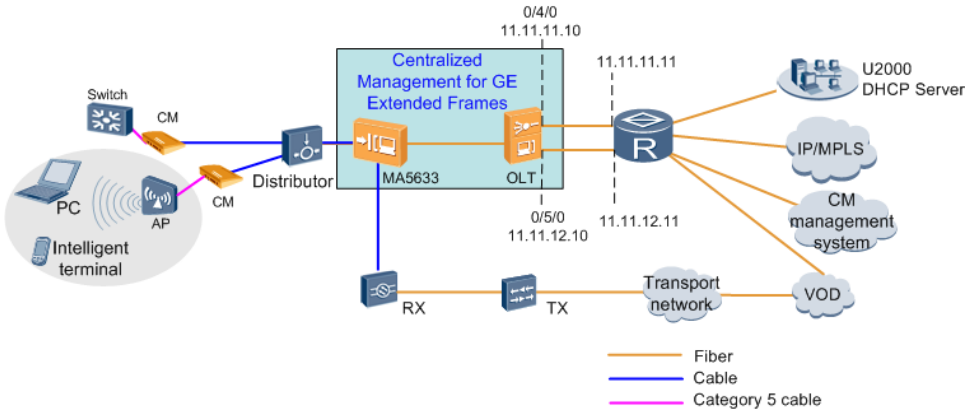
An enterprise requires the provisioning of the L2VPN service.

Usage Scenario

As shown in **Figure 15-15**, an MA5633 is deployed on an optical node and cable modems (CMs) are deployed at enterprises. The CMs connect to radio frequency (RF) ports on the MA5633 through cables.

- A CM provides the enterprise service through a switch, which connects to enterprise users.
- Enterprise users access the Internet through Dynamic Host Configuration Protocol (DHCP) dialup.
- The MA5633 works as a GE remote extended frame to reduce MA5633 management and maintenance costs and simplify configurations.

Figure 15-15 L2VPN enterprise service networking

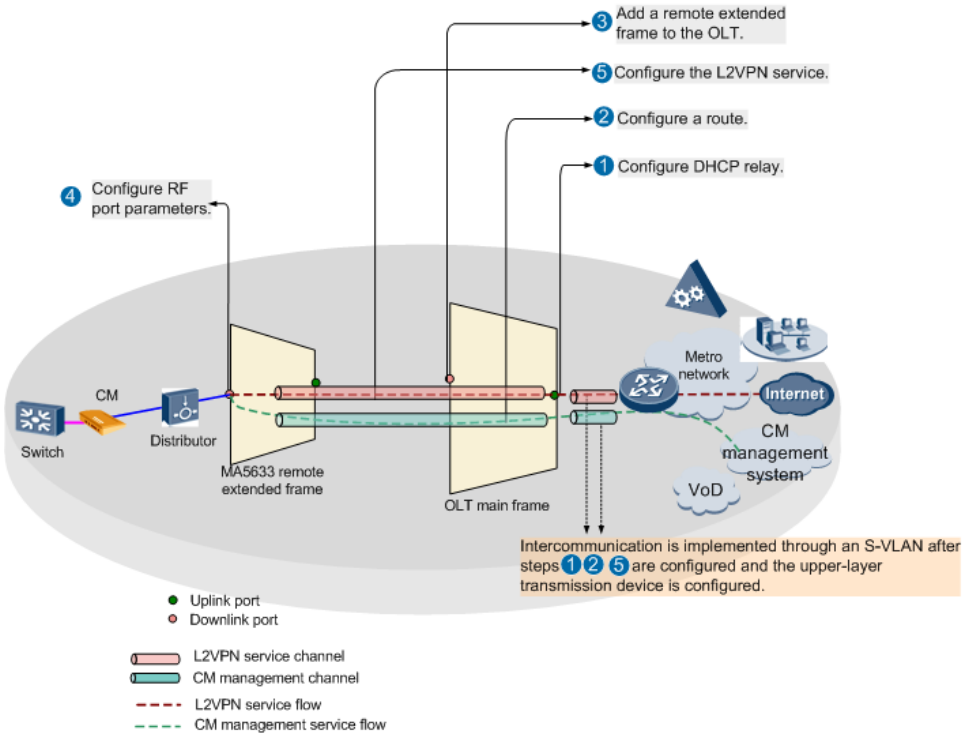


15.4.2.2 Configuration Process

Figure 15-16 shows the configuration roadmap for the L2VPN service networking.

Copyright © Huawei Technologies Co., Ltd.

Figure 15-16 Configuration roadmap for the L2VPN service networking



The following table describes the configuration steps. All configurations are issued from the optical line terminal (OLT).

No.	Step	Description
1	● IPv4: **Configure Dynamic Host Configuration Protocol (DHCP) relay.** ● IPv6: **Configure Dynamic Host Configuration Protocol (DHCP) relay (IPv6).**	This section describes how to configure Dynamic Host Configuration Protocol (DHCP) relay so that cable modems (CMs) can obtain IP addresses in different network segments.
2	● IPv4: **Configure a route.** ● IPv6: **Configure a route (IPv6).**	This section describes how to implement network communication by configuring a route in Layer 3 networking with an optical line terminal (OLT). Through the route, packets are forwarded at Layer 3 between the OLT and its upper-layer devices or servers.
3	**Add a remote extended frame to the OLT.**	An MA5633 that works as a remote extended frame connects to a port on a cascading board of an optical line terminal (OLT). You can configure the remote extended frame only after adding it to the OLT.

Copyright © Huawei Technologies Co., Ltd.

No.	Step	Description
4	**Configure radio frequency (RF) port parameters.**	Radio frequency (RF) port parameters define the frequency spectrum range for signal transmission and modulation mode. The configuration of RF port parameters implements data service transmission over cables. RF port parameters can be configured using either of the following methods: ● Use a cable initialization profile to configure the parameters. ● Customize the parameters in cable mode.
5	**Configure the L2VPN service.**	In the upstream direction, a cable modem (CM) connects to a distributed cable modem termination system (D-CMTS) through a cable. In the downstream direction, the CM connects to a switch to provide the L2VPN enterprise service to the users connected to the switch.
6	**Verify the configured service.**	An OLT supports multiple remote service verification methods. This allows commissioning and configuration engineers to remotely verify services. 1. A DHCP dialup emulation test checks whether the OLT can communicate with the DHCP server and verifies CM DHCP configurations on the DHCP relay, proxy, and server. 2. The status of a CM can be queried. Based on the information, you can determine whether the CM is online.

15.4.2.3 Configuring DHCP Relay

This section describes how to configure Dynamic Host Configuration Protocol (DHCP) relay so that cable modems (CMs) can obtain IP addresses in different network segments.

Prerequisites

The upper-layer router, DHCP server, and Trivial File Transfer Protocol (TFTP) server of an optical line terminal (OLT) have been configured.

Copyright © Huawei Technologies Co., Ltd.

Data Plan

Table 15-43 DHCP data plan for the OLT

Item	Data
VLAN	ID of the CM management S-VLAN: 200; type of the VLAN: smart
DHCP server group parameters	IP address of the DHCP domain gateway for CMs: 10.10.224.1; domain name: docsis

Table 15-44 Data plan for the upper-layer devices of the OLT

Item	IP Address
Layer 3 interfaces connecting the router to the OLT	● Forwarding DHCP and broadband packets: 11.11.11.11 ● Forwarding CM management packets: 11.11.12.11
IP address of the DHCP server	DHCP server assigning IP addresses to CMs and media terminal adapters (MTAs): 192.168.10.10-192.168.10.11

Procedure

Step 1 Set the IP address of the VLAN Layer 3 interface.

```
huawei(config)#vlan 100 smart
huawei(config)#interface vlanif 100
huawei(config-if-vlanif100)#ip address 10.10.224.1 255.255.255.0     //Set the IP address of the DHCP domain gateway for CMs.
huawei(config-if-vlanif100)#quit
```

Step 2 Configure the working mode of the DHCP relay to Layer 3 Option 60.

In DHCP Option 60 mode, a DHCP server group is selected according to the Option 60 domain name in DHCP packets. Users in this mode are identified by domain information of packets, which differentiates various service types in a VLAN. Ensure that the Option 60 domain name and the DHCP server group bound to the Option 60 domain name are configured beforehand.

```
huawei(config)#dhcp mode layer-3 Option60
  Several minutes may be required and no action can be taken during this period
  Are you sure to perform this operation? (y/n)[n]: y
```

Step 3 Set the IP addresses of the servers in a DHCP server group.

```
huawei(config)#dhcp-server 0 ip 192.168.10.10 192.168.10.11    //Configure DHCP server group 0 to assign IP addresses to CMs.
```

Step 4 Create a DHCP Option 60 domain.

```
huawei(config)#dhcp domain docsis   //Create Option 60 domain name docsis for CMs.
huawei(config-dhcp-domain-docsis)#dhcp-server 0 vlan 100       //Bind DHCP server group 0 to the DHCP domain where the CMs locate. After the configuration, the CMs in the DHCP domain are corresponded to DHCP server group 0.
huawei(config-dhcp-domain-docsis)#quit
```


Copyright © Huawei Technologies Co., Ltd.

Step 5 Set the IP address of the gateway for the DHCP domain.

```
huawei(config)#interface vlanif 100
huawei(config-if-vlanif100)#dhcp domain docsis gateway 10.10.224.1    //Set the IP
address of the gateway for the CM domain to 10.10.224.1.
huawei(config-if-vlanif100)#quit
```

----End

15.4.2.4 Configuring a Route

This section describes how to implement network communication by configuring a route in Layer 3 networking with an optical line terminal (OLT). Through the route, packets are forwarded at Layer 3 between the OLT and its upper-layer devices or servers.

Prerequisites

The upper-layer router of an OLT has been configured.

Data Plan

Table 15-45 Data plan for the Layer 3 interfaces on the network side

Item	IP Address
Layer 3 interfaces on the OLT network side	Forwarding Dynamic Host Configuration Protocol (DHCP) packets: ● VLAN ID: 2004 ● Port number: 0/4/0 ● IP address: 11.11.11.10/24 Forwarding cable modem (CM) management packets: ● VLAN ID: 2005 ● Port number: 0/5/0 ● IP address: 11.11.12.10/24
Layer 3 interfaces connecting the router to the OLT	● Forwarding DHCP packets: 11.11.11.11 ● Forwarding CM management packets: 11.11.12.11
Upper-layer servers of the OLT	● DHCP server assigning IP addresses to CMs and media terminal adapters (MTAs): 192.168.10.10-192.168.10.11 ● CM management system: 192.168.20.1

Procedure

Step 1 Create Layer 3 VLAN interfaces on the network side.

1. Create VLANs and configure their uplink ports.
   - VLAN 2004 is of the smart VLAN type and used for forwarding DHCP packets. Add uplink port 0/4/0 to VLAN 2004.

Copyright © Huawei Technologies Co., Ltd.

- VLAN 2005 is of the smart VLAN type and used for forwarding CM management packets. Add uplink port 0/5/0 to VLAN 2005.

```
huawei(config)#vlan 2004 to 2006 smart
huawei(config)#port vlan 2004 0/4 0
huawei(config)#port vlan 2005 0/5 0
```

2. (Optional) Create native VLANs for Ethernet outbound ports.

   Packets between the OLT and its upper-layer router are forwarded at Layer 3 and no VLAN information is required. The created native VLANs remove VLAN tags from the packets transmitted out of Ethernet ports.

```
huawei(config)#interface eth 0/4
huawei(config-if-eth-0/4)#native-vlan 0 vlan 2004    //Remove VLAN tags from
the packets transmitted out of the 0/4/0 port.
huawei(config-if-eth-0/4)#quit
huawei(config)#interface eth 0/5
huawei(config-if-eth-0/5)#native-vlan 0 vlan 2005    //Remove VLAN tags from
the packets transmitted out of the 0/5/0 port.
huawei(config-if-eth-0/5)#quit
```

3. Create Layer 3 VLAN interfaces.

   a. Create a Layer 3 interface for VLAN 2004, through which DHCP packets are forwarded.

```
huawei(config)#interface vlanif 2004
huawei(config-if-vlanif2004)#ip address 11.11.11.10 255.255.255.0
huawei(config-if-vlanif2004)#quit
```

   b. Create a Layer 3 interface for VLAN 2005, through which CM management packets are forwarded.

```
huawei(config)#interface vlanif 2005
huawei(config-if-vlanif2005)#ip address 11.11.12.10 255.255.255.0
huawei(config-if-vlanif2005)#quit
```

Step 2 Configure static routes to implement the communication between the OLT and its upper-layer devices.

```
huawei(config)#ip route-static 192.168.20.0 255.255.255.0 11.11.12.11     //CM
management and VoD packets are forwarded through the Layer 3 interface of VLAN
2005.
huawei(config)#ip route-static 192.168.10.0 255.255.255.0 11.11.11.11     //DHCP
packets are forwarded through the Layer 3 interface of VLAN 2004.
```

NOTE

The interconnected router must set static routes and add the routes to dynamic routes.

----End

Result

The OLT can communicate with its upper-layer devices. To check network connectivity between two devices, run the **ping** and **tracert** commands.

The configured static routes can be queried in an IPv4 routing table by running the **display ip routing-table** command.

15.4.2.5 Configuring DHCP Relay (IPv6)

This section describes how to configure DHCPv6 relay so that CMs can obtain IP addresses in different network segments.

Copyright © Huawei Technologies Co., Ltd.

Prerequisites

The upper-layer router, DHCP server, and Trivial File Transfer Protocol (TFTP) server of an OLT have been configured.

Data Plan

Table 15-46 data plan

Configuration Item	Data
Terminal-side of CM	network segment of CM: 2001:0db8:0001::/64
User-side of OLT	IP address of the gateway for the DHCP domain of CMs: 2001:0db8:0001::1/64; domain name: **docsis**
Network-side of OLT	Forwarding DHCP and broadband packets: ● VLAN ID: 2004 ● Port number: 0/4/0 ● IP address: 2001:0db8:0007::12/64 Forwarding CM management packets, multicast packets, and VoD packets: ● VLAN ID: 2005 ● Port number: 0/5/0 ● IP address: 2001:0db8:0008::13/64
Router	● IP address of the Layer 3 interface for forwarding DHCP and broadband packets: 2001:0db8:0007::6/64 ● IP address of the Layer 3 interface for forwarding CM management packets: 2001:0db8:0008::7/64
Server	● IP addresses of DHCP servers: – DHCP server allocating IP addresses for CMs: 2001:0db8:0006::8/64-2001:0db8:0006::9/64 – DHCP server allocating IP addresses for PCs: 2001:0db8:0006::10/64-2001:0db8:0006::11/64 ● IP addresses of the CM management system: 2001:0db8:0011::14/64-2001:0db8:0011::16/64

Procedure

Step 1 Configure a CM service provisioning mode, which can be IPv6 (preferentially used), APM, or DPM (used for dual-stack service provisioning). Select a mode based on site requirements.

```
huawei(config)#interface cable 1/1/0
huawei(config-if-cable-1/1/0)#cable ip-mode dpm
huawei(config-if-cable-1/1/0)#quit
```

Step 2 Configure the IP address of the VLAN Layer 3 interface.

Copyright © Huawei Technologies Co., Ltd.

```
huawei(config)#ipv6      //Enable IPv6 packet forwarding.
huawei(config)#vlan 100
huawei(config)#interface vlanif 100
huawei(config-if-vlanif100)#ipv6 enable     //Enable IPv6 on ports.
huawei(config-if-vlanif100)#undo ipv6 nd ra halt       //enables a router to send
RA messages.
huawei(config-if-vlanif100)#ipv6 nd autoconfig managed-address-flag     //Configure
the state-based auto-configuration address flag bit. The host obtains an IPv6
address using the state-based automatic configuration.
huawei(config-if-vlanif100)#ipv6 address 2001:0db8:0001::1/64     //Configure the
IP address of the gateway for the DHCP domain of CMs.
huawei(config-if-vlanif100)#quit
```

Step 3 Enable duplicate address detect (DAD) proxy, which prevents repeated link local addresses (LLAs) on the user side.

After receiving a DAD packet sent from the user side with destination IP address LLA, the OLT with DAD proxy enabled checks user online information based on the destination IP address and VLAN. If a user with the same IP address in the VLAN has been online, the OLT makes a response and prohibits the new user from going online. Otherwise, the OLT does not make a response.

```
huawei(config)#ipv6 dad proxy enable
huawei(config)#vlan service-profile profile-id 10
huawei(config)#vlan bind service-profile 100 profile-id 10
huawei(config-vlan-srvprof-10)#ipv6 dad proxy enable     //DAD proxy takes effect
after it is enabled at system level and VLAN service profile level.
```

Step 4 Configure the working mode of DHCP relay to Layer 3 Option 16.

Option 16 is an option with code 16 in DHCPv6 packets, which identifies terminal types. In DHCPv6 Option 16 mode, packets select a DHCPv6 server based on the Option 16 domain. Therefore, in DHCPv6 Option 16 mode, packets select a DHCPv6 server based on terminal types.

```
huawei(config)#dhcpv6 mode layer-3 option16
  Several minutes may be required and no action can be taken during this period
  Are you sure to perform this operation? (y/n)[n]: y
```

Step 5 Configure the IP addresses of the servers in a DHCP server group.

```
huawei(config)#dhcpv6-server 0 ipv6 2001:0db8:0006::8/64 2001:0db8:0006::9/64    //
Configure DHCP server group 0 to allocate IP addresses for CMs.
```

Step 6 Create DHCP Option 16 domains.

```
huawei(config)#dhcp domain docsis   //Create Option 16 domain docsis for CMs.
huawei(config-dhcp-domain-docsis)#dhcpv6-server 0 vlan 100      //Bind DHCP server
group 0 to the DHCP domain of CMs. After the configuration, the CMs in this DHCP
domain are mapped to DHCP server group 0.
huawei(config-dhcp-domain-docsis)#quit
```

Step 7 Configure the IP addresses of the gateways for DHCP domains.

```
huawei(config)#interface vlanif 100
huawei(config-if-vlanif100)#dhcpv6 domain docsis gateway 2001:0db8:0001::1/64    //
Configure the IP address of the gateway for the DHCP domain of CMs.
huawei(config-if-vlanif100)#quit
```

----End

15.4.2.6 Configuring a Route (IPv6)

This section describes how to implement network communication by configuring a route in Layer 3 networking with an OLT. Through the route, the OLT can forward packets at Layer 3 between the OLT and its upper-layer devices or servers.

Copyright © Huawei Technologies Co., Ltd.

Prerequisites

The upper-layer router of the OLT has been configured.

Data Plan

Table 15-47 data plan

Configuration Item	Data
Terminal-side of CM	network segment of CM: 2001:0db8:0001::/64
User-side of OLT	IP address of the gateway for the DHCP domain of CMs: 2001:0db8:0001::1/64; domain name: **docsis**
Network-side of OLT	Forwarding DHCP and broadband packets: ● VLAN ID: 2004 ● Port number: 0/4/0 ● IP address: 2001:0db8:0007::12/64 Forwarding CM management packets, multicast packets, and VoD packets: ● VLAN ID: 2005 ● Port number: 0/5/0 ● IP address: 2001:0db8:0008::13/64
Router	● IP address of the Layer 3 interface for forwarding DHCP and broadband packets: 2001:0db8:0007::6/64 ● IP address of the Layer 3 interface for forwarding CM management packets: 2001:0db8:0008::7/64
Server	● IP addresses of DHCP servers: – DHCP server allocating IP addresses for CMs: 2001:0db8:0006::8/64-2001:0db8:0006::9/64 – DHCP server allocating IP addresses for PCs: 2001:0db8:0006::10/64-2001:0db8:0006::11/64 ● IP addresses of the CM management system: 2001:0db8:0011::14/64-2001:0db8:0011::16/64

Procedure

Step 1 Create VLAN Layer 3 interfaces on the network side.

1. Create VLANs and add an uplink port to them, respectively.
   - VLAN 2004 used for forwarding DHCP packets is a smart VLAN. Add uplink port 0/4/0 to VLAN 2004.
   - VLAN 2005 used for forwarding CM management packets is a smart VLAN. Add uplink port 0/5/0 to VLAN 2005.

Copyright © Huawei Technologies Co., Ltd.

```
huawei(config)#vlan 2004 to 2005 smart
huawei(config)#port vlan 2004 0/4 0
huawei(config)#port vlan 2005 0/5 0
```

2. (Optional) Create native VLANs for Ethernet outbound ports.

   Packets between the OLT and its upper-layer router are forwarded at Layer 3 and no VLAN tag is required. The created native VLANs remove VLAN tags from the packets transmitted out of Ethernet ports.

```
huawei(config)#interface eth 0/4
huawei(config-if-eth-0/4)#native-vlan 0 vlan 2004    //The packets transmitted
out of port 0/4/0 are untagged.
huawei(config-if-eth-0/4)#quit
huawei(config)#interface eth 0/5
huawei(config-if-eth-0/5)#native-vlan 0 vlan 2005    //The packets transmitted
out of port 0/5/0 are untagged.
huawei(config-if-eth-0/5)#quit
```

3. Create VLAN Layer 3 interfaces.

   a. Create the Layer 3 interface of VLAN 2004, through which DHCP packets are forwarded.

```
huawei(config)#interface vlanif 2004
huawei(config-if-vlanif2004)#ipv6 address 2001:0db8:0007::12/64
huawei(config-if-vlanif2004)#quit
```

   b. Create the Layer 3 interface of VLAN 2005, through which CM management packets are forwarded.

```
huawei(config)#interface vlanif 2005
huawei(config-if-vlanif2005)#ipv6 address 2001:0db8:0008::13/64
huawei(config-if-vlanif2005)#quit
```

Step 2 Configure static routes for the communication between the OLT and its upper-layer devices.

```
huawei(config)#ipv6 route-static 2001:0db8:0006::/64 2001:0db8:0008::7/64     //CM
management packets are forwarded through the Layer 3 interface of VLAN 2005.
huawei(config)#ipv6 route-static 2001:0db8:0011::/64 2001:0db8:0007::6/64     //
DHCP packets are forwarded through the Layer 3 interface of VLAN 2004.
```

NOTE

Configure static routes on the router connected to the OLT. In addition, add the static routes to dynamic ones.

----End

Result

The OLT can communicate with its upper-layer devices. To check network connectivity between two devices, run the **ping ipv6** and **tracert ipv6** commands.

The configured static routes can be queried in an IPv6 routing table by running the **display ipv6 routing-table** command.

15.4.2.7 Adding a Remote Extended Frame to an OLT

A distributed cable modem termination system (D-CMTS) that works as a GE remote extended frame connects to a port on a GE cascading board of an optical line terminal (OLT). You can configure the remote extended frame only after adding it to the OLT.

Copyright © Huawei Technologies Co., Ltd.

Prerequisites

The D-CMTS management policy is set to **extend-frame**. To do so, run the **sysman centralized-mgmt primary** command.

Context

You can use either of the methods listed in the following table to add a remote extended frame to an OLT based on site requirements.

Table 15-48 Methods of adding a remote extended frame to an OLT

Method	Usage Scenario	Remarks
Add a remote extended frame in offline mode.	The remote extended frames must be deployed one by one. This method facilitates remote extended frame management.	The remote extended frame ID has been planned.
Add an automatically discovered remote extended frame.	A great number of remote extended frames need to be deployed. This method reduces manual configurations.	The remote extended frame ID does not need to be planned.

Data Plan

Table 15-49 Data plan

Item	Data
GE cascading board	Board: H801ETHB Port ID: 0/3/1 Remote extended frame ID: 1 **NOTE** The OLT uses the MA5603T as an example. The configuration method is the same for other OLTs. The only difference lies in slot IDs.

Procedure

- Add a remote extended frame in offline mode.

```
huawei(config)#interface eth 0/3
huawei(config-if-eth-0/3)#network-role extend
  This operation will reset the board. Are you sure to continue ? (y/n)[n]:y
huawei(config-if-eth-0/3)#quit
huawei(config)#frame add 1 MA5633 extending-port 0/3/1
```

- Add an automatically discovered remote extended frame.

Copyright © Huawei Technologies Co., Ltd.

The OLT supports the adding of an automatically discovered GE remote extended frame. This function does not require manual confirmation, thereby simplifying the remote extended frame registration and adding flow.

```
huawei(config)#interface eth 0/3
huawei(config-if-eth-0/3)#network-role extend
  This operation will reset the board. Are you sure to continue ? (y/n)[n]:y
huawei(config-if-eth-0/3)#quit
```

----End

Result

The remote extended frame is online.

After adding the remote extended frame, run the **display frame info** command to query the remote extended frame status. Ensure that **Online state** is **online** and **State** is **normal**.

```
huawei(config)#display frame info 1
  ---------------------------------------------------------------------------
  Type:           MA5633
  State:          Normal
  Desc:           MA5633_1_extending_0/3/1
  Hardware:       MA5633
  Extend type:    ETH
  Extending port: 0 /3 /1   //The cascading port on the OLT is 0/3/1.
  Extended port:  1 /0 /0   //The ID of the remote extended frame is 1 and the uplink
port on the remote extended frame is 0/0/0.
  Online state:   Online
  MAC address:    60DE-447D-8711
  ---------------------------------------------------------------------------
```

Follow-up Procedure

If the remote extended frame cannot be discovered, follow the troubleshooting suggestions listed in the following table to rectify faults.

Possible Cause	Troubleshooting Suggestion
The D-CMTS works as a standalone NE and cannot work as a remote extended frame.	Replace the D-CMTS with the one that works as a remote extended frame.
The D-CMTS management policy is set to **stand-alone** on the OLT.	Run the **sysman centralized-mgmt primary** command to configure the D-CMTS management policy to **extend-frame**.
The number of remote extended frames on the OLT has reached the threshold.	Run the **frame delete** command to delete a remote extended frame that is no longer used from the OLT.
The working mode of the ports on the remote extended frame is not **extend**.	In Ethernet mode, run the **network-role extend** command to set the working mode of the ports to **extend**.

Copyright © Huawei Technologies Co., Ltd.

15.4.2.8 Configuring RF Port Parameters

Radio frequency (RF) port parameters define the frequency spectrum range for signal transmission and modulation mode. The configuration of RF port parameters implements data service transmission over cables.

Context

You can use either of the methods listed in the following table to configure RF port parameters based on site requirements.

Table 15-50 Methods of configuring RF port parameters

Method	Usage Scenario	Remarks
Use a cable initialization profile to configure RF port parameters.	A carrier needs to deploy remote extended frames in batches. This method reduces data configuration for remote extended frames, thereby improving service provisioning efficiency. Configure the RF parameter profile for the remote extended frames on the optical line terminal (OLT). After the remote extended frames are powered on and added to the OLT, the OLT automatically issues the RF parameter profile to the remote extended frames, without requiring any software configuration. **NOTE** After the cable initialization profile is configured, a remote extended frame uses the RF port parameters configured in the profile after going online, regardless of whether the remote extended frame in added in offline mode or automatically discovered by the OLT.	● If the RF port parameters are the same for all the remote extended frames to be deployed in batches, use the cable initialization profile to configure the parameters. ● If the RF port parameters are basically the same for all the remote extended frames to be deployed in batches, use the cable initialization profile to configure the parameters. Then modify parameter settings in customized cable configuration mode.
Customize RF port parameters in cable mode.	Requires differentiated plans and configurations for RF port parameters of remote extended frames and the remote extended frames must be configured one by one.	If the RF port parameters are greatly different for the remote extended frames to be deployed in batches, use this method to configure the parameters.

Copyright © Huawei Technologies Co., Ltd.

Data Plan

Table 15-51 Data plan for RF port parameters

Item	Data
RF port	1/1/0
Upstream channels	● IDs: 1-4 ● Type: European standard (default channel type) ● ID of the upstream channel modulation profile: 1 (by default) ● Channel central frequency (MHz): 29.8, 42.60, 49.00, and 55.4
Downstream channels	● IDs: 1-16 ● Type: European standard (default channel type) ● Channel central frequency (MHz): 602.00, 610.00, 618.00, ..., and 722.00

Procedure

- Use a cable initialization profile to configure RF port parameters.
  1. Configure the frequency spectrum range and channel type.

     In this example, the channel is of the European type. To change the type to North American, run the **cable** command.
  2. Configure RF port parameters for upstream channels and activate the upstream channels.

Parameter	Description
frequency and **channel-width**	A central frequency and a frequency bandwidth determine a frequency range, within which packets are transmitted. For example, the central frequency of a European channel is 55 MHz and the frequency bandwidth is 6400 kHz. Then the frequency range of the channel is 51.8-58.2 MHz.
modulation-profile	An upstream channel modulation profile defines parameters for processing the signals transmitted over the upstream channel. You do not need to configure an upstream channel modulation profile generally. Ports automatically bind to profile 1 by default.

The following configurations are used as an example to configure RF parameters for upstream channels:

Copyright © Huawei Technologies Co., Ltd.

- Number of upstream channels: 4
- Frequency bandwidth of the channels: 3.2 MHz (default value)

```
huawei(config)#interface cable init-template
huawei(config-cable-init-template)#cable upstream 1 frequency 29.8 enable
huawei(config-cable-init-template)#cable upstream 2 frequency 42.60
enable
huawei(config-cable-init-template)#cable upstream 3 frequency 49.00
enable
huawei(config-cable-init-template)#cable upstream 4 frequency 55.40
enable
```

3. Configure RF port parameters for downstream channels and activate the downstream channels.

Parameter	Description
modulation	A greater modulation mode value for downstream channels results in a higher channel bandwidth but weaker anti-interference capability. Therefore, configure the modulation mode based on site requirements. The default modulation mode is QAM256. This example uses the default setting.

The following configuration is used as an example to configure RF parameters for downstream channels: A total of 16 downstream channels have been purchased.

```
huawei(config-cable-init-template)#cable downstream 1 frequency 602.00
enable
huawei(config-cable-init-template)#cable downstream 2 frequency 610.00
enable
huawei(config-cable-init-template)#cable downstream 3 frequency 618.00
enable
huawei(config-cable-init-template)#cable downstream 4 frequency 626.00
enable
huawei(config-cable-init-template)#cable downstream 5 frequency 634.00
enable
huawei(config-cable-init-template)#cable downstream 6 frequency 642.00
enable
huawei(config-cable-init-template)#cable downstream 7 frequency 650.00
enable
huawei(config-cable-init-template)#cable downstream 8 frequency 658.00
enable
huawei(config-cable-init-template)#cable downstream 9 frequency 666.00
enable
huawei(config-cable-init-template)#cable downstream 10 frequency 674.00
enable
huawei(config-cable-init-template)#cable downstream 11 frequency 682.00
enable
huawei(config-cable-init-template)#cable downstream 12 frequency 690.00
enable
huawei(config-cable-init-template)#cable downstream 13 frequency 698.00
enable
huawei(config-cable-init-template)#cable downstream 14 frequency 706.00
enable
huawei(config-cable-init-template)#cable downstream 15 frequency 714.00
enable
```


Copyright © Huawei Technologies Co., Ltd.

```
huawei(config-cable-init-template)#cable downstream 16 frequency 722.00
enable
```

- Customize the RF port parameters in cable mode.

  NOTE

  The configuration is complete if you have configured the RF port parameters using a cable initialization profile. For details, see **Use a cable initialization profile to configure RF port parameters**. Perform this operation if you need to customize the RF port parameters of a remote extended frame.

  1. Configure RF port parameters for upstream channels and activate the upstream channels.

     ```
     huawei(config)#interface cable 1/1/0
     huawei(config-if-cable-1/1/0)#cable upstream 1 frequency 29.8 enable
     huawei(config-if-cable-1/1/0)#cable upstream 2 frequency 42.60 enable
     huawei(config-if-cable-1/1/0)#cable upstream 3 frequency 49.00 enable
     huawei(config-if-cable-1/1/0)#cable upstream 4 frequency 55.40 enable
     ```

  2. Configure RF port parameters for downstream channels and activate the downstream channels.

     ```
     huawei(config-if-cable-1/1/0)#cable downstream 1 frequency 602.00 enable
     huawei(config-if-cable-1/1/0)#cable downstream 2 frequency 610.00 enable
     huawei(config-if-cable-1/1/0)#cable downstream 3 frequency 618.00 enable
     huawei(config-if-cable-1/1/0)#cable downstream 4 frequency 626.00 enable
     huawei(config-if-cable-1/1/0)#cable downstream 5 frequency 634.00 enable
     huawei(config-if-cable-1/1/0)#cable downstream 6 frequency 642.00 enable
     huawei(config-if-cable-1/1/0)#cable downstream 7 frequency 650.00 enable
     huawei(config-if-cable-1/1/0)#cable downstream 8 frequency 658.00 enable
     huawei(config-if-cable-1/1/0)#cable downstream 9 frequency 666.00 enable
     huawei(config-if-cable-1/1/0)#cable downstream 10 frequency 674.00 enable
     huawei(config-if-cable-1/1/0)#cable downstream 11 frequency 682.00 enable
     huawei(config-if-cable-1/1/0)#cable downstream 12 frequency 690.00 enable
     huawei(config-if-cable-1/1/0)#cable downstream 13 frequency 698.00 enable
     huawei(config-if-cable-1/1/0)#cable downstream 14 frequency 706.00 enable
     huawei(config-if-cable-1/1/0)#cable downstream 15 frequency 714.00 enable
     huawei(config-if-cable-1/1/0)#cable downstream 16 frequency 722.00 enable
     ```

----End

Result

1. The transmit power of the downstream channels meets site requirements.

   Run the **display cable downstream** *frameid/slotid/portid* { **all** | *channel-id* } **status** command to check whether the RF port parameters meet site requirements.

2. The signal-to-noise (SNR) ratio of the upstream channels meets site requirements.

   Run the **display cable signal quality** [*frameid/slotid/portid* [**upstream** *channel-id*]] command to check whether the RF port parameters meet site requirements. A greater SNR ratio results in better signal quality. The recommended SNR ratio is greater than 30 dB.

15.4.2.9 Configuring the L2VPN Enterprise Service

In the upstream direction, a cable modem (CM) connects to a distributed cable modem termination system (D-CMTS) through a cable. In the downstream direction, the CM connects to a switch to provide the L2VPN enterprise service to the users connected to the switch.

Copyright © Huawei Technologies Co., Ltd.

Context

An L2VPN S-VLAN can be configured through a CM configuration file or commands. Only one mode is used each time generally. If both modes are used, the S-VLAN configuration through commands preferentially takes effect on the system when the CM goes online.

- S-VLAN configuration through a CM configuration file: Run the **vlan** command to add a CM S-VLAN and run the **port vlan** command to add the uplink port for the CM to the S-VLAN. The L2VPN S-VLAN is specified in the CM configuration file. When the CM goes online, the system obtains the L2VPN S-VLAN from the CM configuration file and automatically creates L2VPN service flows.
- S-VLAN configuration through commands: Manually configure the L2VPN S-VLAN on the system. For details, see the following procedure.

Data Plan

Table 15-52 Data plan for the L2VPN service

Item	Data
VLAN	ID of the L2VPN S-VLAN: 200; type of the VLAN: smart
Uplink ports	Port forwarding Dynamic Host Configuration Protocol (DHCP) and broadband packets: 0/4/0 Port forwarding CM management packets: 0/5/0

Procedure

Step 1 Create an L2VPN S-VLAN and add the uplink port to it.

The ID of the L2VPN S-VLAN is 200 and the type of the VLAN is smart. Uplink port 0/4/0 is added to S-VLAN 200.

When the L2VPN S-VLAN is configured through commands, the ID of the L2VPN VLAN is 200 for the CM with MAC address 0000-0000-1111 connected to port 1/1/0.

- To configure the L2VPN S-VLAN through a CM configuration file, run the following commands:

```
huawei(config)#vlan 200 smart
huawei(config)#port vlan 200 0/4 0
```

- To configure the L2VPN S-VLAN through commands, run the following commands:

```
huawei(config)#vlan 200 smart
huawei(config)#cable l2vpn dot1q 1/1/0 cm 0000-0000-1111 200
huawei(config)#port vlan 200 0/4 0
```

Step 2 Configure a VLAN service profile and set the DHCP forwarding mode for VLAN 200 to Layer 2 forwarding.

```
huawei(config)#vlan service-profile profile-name l2vpn
huawei(config-vlan-srvprof-1)#dhcp mode layer-2
huawei(config-vlan-srvprof-1)#commit
huawei(config-vlan-srvprof-1)#quit
huawei(config)#vlan bind service-profile 200 profile-name l2vpn
```

----End

Copyright © Huawei Technologies Co., Ltd.

15.4.2.10 Verifying Services

A distributed cable modem termination system (D-CMTS) working as a remote extended frame locates on an optical node. To facilitate service verification, the optical line terminal (OLT) supports multiple remote service verification methods, such as Dynamic Host Configuration Protocol (DHCP) dialup emulation tests. This allows commissioning and configuration engineers to remotely verify services. In addition, this section describes how to verify the L2VPN service on site.

Prerequisites

- The OLT is properly connected to the upper-layer network.
- The DHCP server, Trivial File Transfer Protocol (TFTP) server, and softswitch or IP multimedia subsystem (IMS) have been configured.

Procedure

- Perform a DHCP dialup emulation test.

  In this test, a cable modem (CM) is emulated on the OLT to apply to the DHCP server for an IP address. This checks whether the OLT can communicate with the DHCP server and verifies CM DHCP configurations on the DHCP relay, proxy, and server.

  1. Run the **simulate dhcp start cm** *mac-address* [**option60** *option60*] command to start a DHCP dialup emulation test.

     NOTE

     You can run the **simulate dhcp stop** command to stop the DHCP emulation.

  2. Run the **display simulation dhcp** command to query the results of the DHCP dialup emulation test.
  3. Check whether the **User IP** has obtained an IP address.

- Check the CM status.

  Run the **display cable modem** command to query the CM status in **Status**.

```
huawei(config)#display cable modem  all

------------------------------------------------------------------------------
-
 Idx   MAC            IP              I/F          Status   Prim  Num Ver  DS
RX
                                                           SID   CPE
Power

------------------------------------------------------------------------------
-
 1     0023-ED6F-21A3 192.168.1.118   1/1/0/U4     ol-pt    1     0   D2.0
-

------------------------------------------------------------------------------
-
 Total:
1
 ol: 0, ol-ptd: 0, ol-pt: 1, ol-d: 0, wol: 0, wol-ptd: 0, wol-pt: 0, wol-d:
0,
pol: 0, pol-ptd: 0, pol-pt: 0, pol-d: 0, offline: 0, rej-m: 0, rej-pt: 0, rej-
o:
 0, init: 0, init-rc: 0, DHCP: 0, DHCP-O: 0, DHCP-R: 0, DHCP-C: 0, REG:
```


Copyright © Huawei Technologies Co., Ltd.

```
0
 Note: 1. Idx is the index of a
CM.
       2. The downstream received power is in the unit of
dBmV.
       3. In status, "ol" means online, "rej" means reject.
```

The following table lists the CM status and handling suggestions.

CM Status	Description	Handling Suggestion
init	Indicates that the CM initialization ranging message is received.the CM initialization.	If a CM is always in the ranging state, the ranging fails. Then check radio frequency (RF) line indicators and detect line faults.
init-rc	Indicates that the CM initialization ranging is complete.	No action is required. The ranging of the CM is complete.
DHCP	Indicates that the DHCP discovery from the CM is received.	If a CM initiates a DHCP request but does not obtain an IP address, check the DHCP server, routing between the OLT and the DHCP server, and DHCP server parameter settings.
● DHCP-O ● DHCP-R ● DHCP-C	● DHCP-O: indicates that the offer from the DHCP server is received. ● DHCP-R: indicates that the DHCP request from the CM is received. ● DHCP-C: indicates that the acknowledge from the DHCP server is received.	The DHCP server has assigned an IP address to the CM and sent configuration file name and IP address of the TFTP or ToD server to the CM using the Option 67 and Option 66 fields (the Option 67 field carries the configuration file name and the Option 66 field carries the IP address of the TFTP or ToD server). If the CM is always in the DHCP-C state, the CM fails to obtain the configuration file. Then check the TFTP server, routing between the OLT and the TFTP server, and TFTP server parameter settings.
REG	Indicates that a registration is started.	If the CM is always in the register state, the CM obtains an incorrect configuration file. Then change the configuration file.

Copyright © Huawei Technologies Co., Ltd.

CM Status	Description	Handling Suggestion
● ol ● ol-pt ● ol-ptd ● ol-d ● wol ● wol-pt ● wol-ptd ● wol-d ● pol ● pol-pt ● pol-ptd	● ol: indicates that the CM is online. (valid only for CMs complying with DOCSIS 2.0) ● ol-pt: indicates that the CM is online and passes the BPI authentication. (valid only for CMs complying with DOCSIS 2.0) ● ol-ptd: indicates that the CM is online and passes the BPI authentication, and NetAccessEnable is disabled. (valid only for CMs complying with DOCSIS 2.0) ● ol-d: indicates that the CM is online and NetAccessEnable is disabled. (valid only for CMs complying with DOCSIS 2.0) ● wol: indicates that the CM is online and all channels bound to the CM are available. (valid only for CMs complying with DOCSIS 3.0) ● wol-pt: indicates that the CM is online and passes the BPI authentication, and all channels bound to the CM are available. (valid only for CMs complying with DOCSIS 3.0) ● wol-ptd: indicates that the CM is online and passes the BPI authentication, NetAccessEnable is disabled, and all channels bound to the CM are available. (valid only for CMs complying with DOCSIS 3.0) ● wol-d: indicates that the CM is online, NetAccessEnable is disabled, and all channels bound to the CM are available. (valid only for CMs complying with DOCSIS 3.0) ● pol: indicates that the CM is online and some channels	No action is required. The status indicates that the CM has registered

Copyright © Huawei Technologies Co., Ltd.

CM Status	Description	Handling Suggestion
● pol-d	bound to the CM are available. (valid only for CMs complying with DOCSIS 3.0) ● pol-pt: indicates that the CM is online and passes the BPI authentication, and some channels bound to the CM are available. (valid only for CMs complying with DOCSIS 3.0) ● pol-ptd: indicates that the CM is online and passes the BPI authentication, NetAccessEnable is disabled, and some channels bound to the CM are available. (valid only for CMs complying with DOCSIS 3.0) ● pol-d: indicates that the CM is online, NetAccessEnable is disabled, and some channels bound to the CM are available. (valid only for CMs complying with DOCSIS 3.0)	with the OLT and can correctly transmit and receive services.
offline	Indicates the offline status.	If the CM is in the offline state, check the power status, noise, and channel frequency of the CM.
● rej-m ● rej-pt ● rej-o	● rej-m: indicates that the MIC verification fails. ● rej-pt: indicates that the BPI authentication fails. ● rej-o: indicates that the authentication reject due to other reasons.	If the CM is in the reject state, no service flow can be created. Then check the CM authentication and CM message integrity check (MIC), and check whether class of service (COS) parameters specified in the CM configuration file are supported by the OLT.

- Verify that the L2VPN service can be provisioned.
  After the CM is installed in the enterprise and the switch connected to the CM is commissioned, L2VPN service can be provisioned.

----End

15.4.3 WLAN Hotspot Radio Backhaul Service Networking

In wireless local area network (WLAN) hotspot radio backhaul service networking, a distributed cable modem termination system (D-CMTS) connects to cable modems (CMs) through radio frequency (RF) ports. A CM connects to wireless access points (APs) to provide wireless fidelity

Copyright © Huawei Technologies Co., Ltd.

(Wi-Fi) access for users. This section describes how to configure the optical line terminal (OLT) to provision the WLAN hotspot radio backhaul service.

Service Requirements

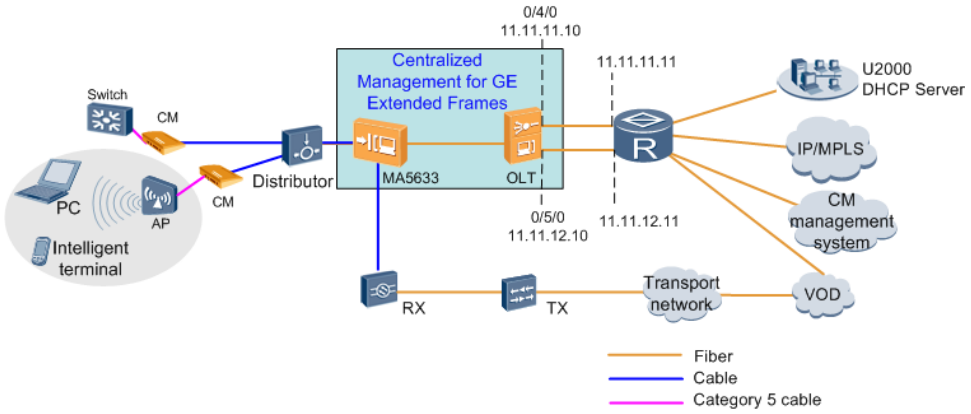
A network supplier needs to provide the Internet access service through Wi-Fi for a business area covered by APs.

Usage Scenario

As shown in **Figure 15-17**, a D-CMTS is deployed on an optical node and CMs are deployed at shops. The CMs connect to RF ports on the D-CMTS through cables.

- A CM connects to wireless APs to provide the WLAN hotspot radio backhaul service. The wireless APs provide Wi-Fi access for users.
- Wi-Fi users access the Internet through Dynamic Host Configuration Protocol (DHCP) dialup.
- The D-CMTS works as a GE remote extended frame. This reduces D-CMTS management and maintenance costs and simplifies configurations.

Figure 15-17 WLAN hotspot radio backhaul service networking



Configuration

The method of configuring the WLAN hotspot radio backhaul service is the same as that of configuring the L2VPN enterprise service and therefore is not described in this section. For details, see **15.4.2.2 Configuration Process**.

15.5 Service Configuration on a D-CMTS That Works as a GPON Remote Extended Frame on a Layer 2 Telecom Network

This section describes how to configure services, including home services, L2VPN enterprise service, and wireless local area network (WLAN) hotspot radio backhaul service, on an optical

Copyright © Huawei Technologies Co., Ltd.

line terminal (OLT) when a distributed cable modem termination system (D-CMTS) works as a GPON extended frame on a Layer 2 telecom network. The MA5603T equipped with the SCUV, GPMD, and SPUF boards is used as an example.

Control Board	SCUV
Cascading Board	GPMD: 0/3
SPU Board	SPUF: 0/4, 0/5

15.5.1 Home Service Networking

In home service (VLAN tag transparent transmission) networking, a distributed cable modem termination system (D-CMTS) connects to cable modems (CMs) at user homes through radio frequency (RF) ports and provides home services for users, including the cable TV (CATV) service, Internet access service, and VoD service. This section describes how to configure the optical line terminal (OLT) to provision the home services.

15.5.1.1 Service Requirements and Usage Scenario

Service Requirements

Users require the provisioning of the broadcast and TV services, Internet access service, and VoD service. Broadcast and TV services can be provisioned immediately after the distributed cable modem termination system (D-CMTS) hardware is connected. This section only describes how to configure the Internet access service, and VoD service.

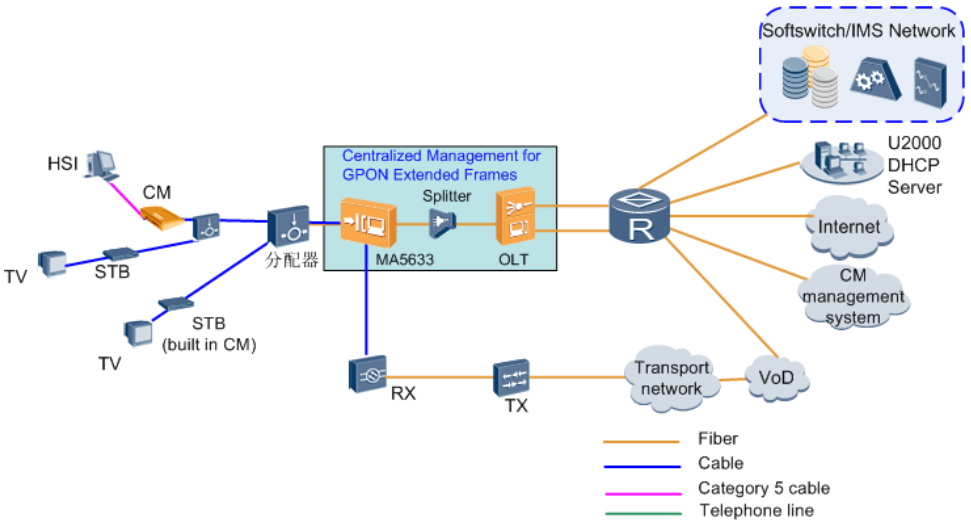
Usage Scenario

As shown in **Figure 15-18**, a D-CMTS is deployed on an optical node and cable modems (CMs) are deployed at user homes. The CMs connect to radio frequency (RF) ports on the MA5633 through cables.

- Port 1 on CM connects to a PC to provide the Internet access service. A set top box (STB) connects to the distributor to provide a backhaul channel for the VoD service.
- Users access the Internet through Dynamic Host Configuration Protocol (DHCP) dialup.
- The IP addresses of the CM, STB, and PC are assigned by the DHCP server and in different network segments.
- The D-CMTS is used as a GPON remote extended frame. This reduces D-CMTS management and maintenance costs and simplifies configurations.

Copyright © Huawei Technologies Co., Ltd.

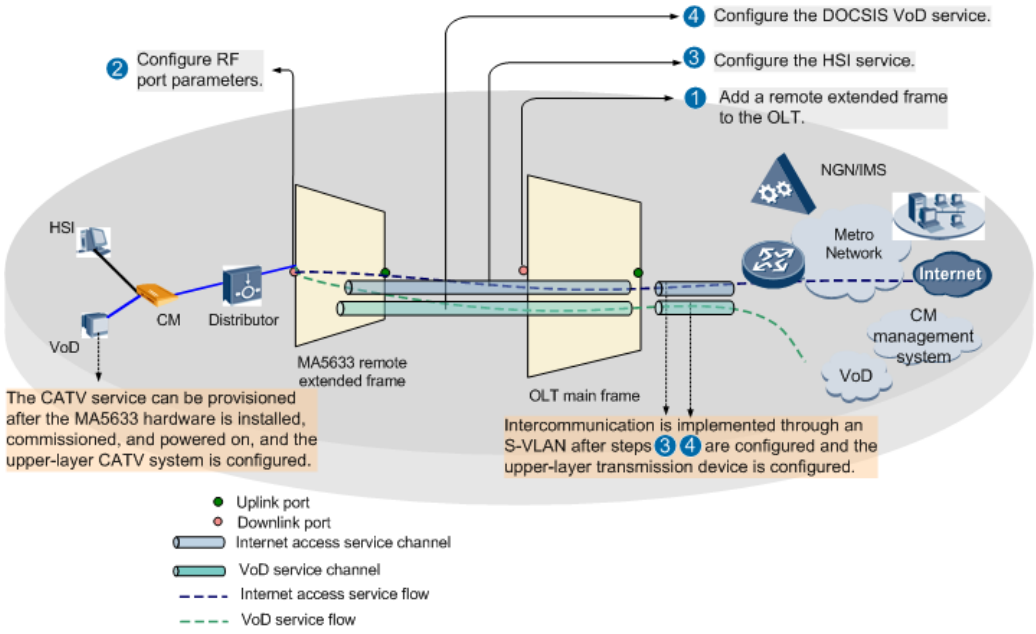
Figure 15-18 Home service networking (VLAN tag transparent transmission)



15.5.1.2 Configuration Process

Figure 15-19 shows the configuration roadmap for the home service networking.

Figure 15-19 Configuration roadmap for the home service networking



The following table describes configuration steps. All configurations are issued from the optical line terminal (OLT).

Copyright © Huawei Technologies Co., Ltd.

No.	Step	Description
1	**Add a remote extended frame to the OLT.**	An MA5633 that works as a remote extended frame connects to a port on a cascading board of an optical line terminal (OLT). You can configure the remote extended frame only after adding it to the OLT.
2	**Configure radio frequency (RF) port parameters.**	Radio frequency (RF) port parameters define the frequency spectrum range for signal transmission and modulation mode. The configuration of RF port parameters implements data service transmission over cables. RF port parameters can be configured using either of the following methods: ● Use a cable initialization profile to configure the parameters. ● Customize the parameters in cable mode.
3	**Configure the high-speed Internet (HSI) service.**	None
4	**Configure the DOCSIS VoD service.**	● If the MA5633 is not equipped with a built-in EQAM module, the MA5633 uses DOCSIS channels to transmit VoD data. ● If the MA5633 is equipped with a built-in EQAM module, the MA5633 sets idle downstream DOCSIS channels as EQAM channels to transmit VoD data. The DOCSIS VoD service and the EQAM VoD service are generally not concurrently used. The DOCSIS VoD service is used as an example.
5	**Verify the configured services.**	An OLT supports multiple remote service verification methods. This allows commissioning and configuration engineers to remotely verify services. 1. A DHCP dialup emulation test checks whether the OLT can communicate with the DHCP server and verifies CM DHCP configurations on the DHCP relay, proxy, and server. 2. The status of a CM can be queried. Based on the information, you can determine whether the CM is online.

Copyright © Huawei Technologies Co., Ltd.

15.5.1.3 Adding a Remote Extended Frame to an OLT

An MA5633 that works as a remote extended frame connects to a port on a cascading board of an optical line terminal (OLT). You can configure the remote extended frame only after adding it to the OLT.

Prerequisites

The MA5633 management policy is set to **extend-frame**. To do so, run the **sysman centralized-mgmt primary** command.

Context

A GPON remote extended frame is added to an OLT in the following two steps: Add the MA5633 to the OLT as a GPON optical network unit (ONU). Then add the MA5633 to the OLT as a GPON remote extended frame.

You can use either of the methods listed in the following table to add a remote extended frame to an OLT based on site requirements.

Table 15-53 Methods of adding a remote extended frame to an OLT

Method	Usage Scenario	Remarks
Add a remote extended frame in offline mode.	A carrier has planned all remote extended frame IDs together and the remote extended frames must be deployed one by one. This method facilitates remote extended frame management.	1. You have obtained the serial number (SN) of the remote extended frame. 2. The remote extended frame ID has been planned.
Add an automatically discovered remote extended frame.	A great number of remote extended frames need to be deployed. This method reduces manual configurations.	1. You do not know the SN of the remote extended frame. 2. The remote extended frame ID does not need to be planned.

Copyright © Huawei Technologies Co., Ltd.

Data Plan

Table 15-54 Data plan

Item	Data
GPON cascading board	Board: H801GPMD Port ID: 0/3/1 Remote extended frame ID: 1 Remote extended frame authentication mode: SN Remote extended frame SN: 48575443E6D8B541 **NOTE** The OLT uses the MA5603T as an example. The configuration method is the same for other OLTs. The only difference lies in slot IDs.
Dynamic bandwidth allocation (DBA)	Profile: default Type: type4 Maximum bandwidth: 1000 Mbit/s
Line profile	Profile: default GPON encapsulation mode (GEM) port ID: 0 (fixed port in centralized management mode) Transmission container (T-CONT) ID: 1 (fixed T-CONT in centralized management mode)
MA5633 management mode	extend-frame

Procedure

- Configure the working mode of the DHCP layer 2 forwarding mode.

  ```
  huawei(config)#dhcp mode layer-2
  ```

- Enable the DHCP option82 feature.

  The DHCP feature does not have any mechanism for authentication or security. Thus, the DHCP feature encounters many security problems when it is used in the network. To solve these problems, the DHCP option82 is introduced.

  ```
  huawei(config)#dhcp option82 enable
  ```

- Add a remote extended frame in offline mode.

  ```
  huawei(config)#frame add 1 MA5633 extending-port 0/3/1 sn 48575443E6D8B541
  ```

  NOTE

  When running the **frame add** command to add a remote extended frame in offline mode, the OLT automatically allocates a temporary SN for the remote extended frame. Therefore, you do not need to specify the SN of the remote extended frame. After obtaining the SN of the remote extended frame, run the **frame bind** command to add the binding relationship between the SN and the remote extended frame to the OLT. Then the remote extended frame is added.

Copyright © Huawei Technologies Co., Ltd.

- Add an automatically discovered remote extended frame.

  The OLT supports the adding of an automatically discovered GPON remote extended frame. This function does not require manual confirmation, thereby simplifying the remote extended frame registration and adding flow.

  ```
  huawei(config)#interface gpon 0/3
  huawei(config-if-gpon-0/3)#port 1 ont-auto-find enable
  huawei(config-if-gpon-0/3)#quit
  ```

----End

Result

The remote extended frame is online.

After adding the remote extended frame, run the **display frame info** command to query the status of the remote extended frame. Ensure that **Online state** is **online** and **State** is **normal**.

```
huawei(config)#display frame info 1
  ---------------------------------------------------------------------------
  Type:           MA5633
  State:          Normal
  Desc:           MA5633_1_extending_0/3/1/1
  Hardware:       MA5633
  Extend type:    GPON
  Extending port: 0 /3 /1
  ONT ID:         1
  ONT SN:         48575443E6D8B541
  Extended port:  1 /0 /1
  Online state:   Online
  Optical-receiver: Offline
  ---------------------------------------------------------------------------
```

Follow-up Procedure

If the remote extended frame cannot be discovered, follow the troubleshooting suggestions listed in the following table to rectify faults.

Possible Cause	Troubleshooting Suggestion
The MA5633 automatic discovery function is disabled.	In GPON mode, run the **port ont-auto-find** command to enable the MA5633 automatic discovery function on GPON ports.
The MA5633 works as a standalone NE and cannot work as a remote extended frame.	Replace the MA5633 with the one that works as a remote extended frame.
The MA5633 management policy is set to **stand-alone** on the OLT.	Run the **sysman centralized-mgmt primary** command to configure the MA5633 management policy to **extend-frame**.
The number of remote extended frames on the OLT has reached the threshold.	Run the **frame delete** command to delete a remote extended frame that is no longer used from the OLT.

Copyright © Huawei Technologies Co., Ltd.

15.5.1.4 Configuring RF Port Parameters

Radio frequency (RF) port parameters define the frequency spectrum range for signal transmission and modulation mode. The configuration of RF port parameters implements data service transmission over cables.

Context

You can use either of the methods listed in the following table to configure RF port parameters based on site requirements.

Table 15-55 Methods of configuring RF port parameters

Method	Usage Scenario	Remarks
Use a cable initialization profile to configure RF port parameters.	A carrier needs to deploy remote extended frames in batches. This method reduces data configuration for remote extended frames, thereby improving service provisioning efficiency. Configure the RF parameter profile for the remote extended frames on the optical line terminal (OLT). After the remote extended frames are powered on and added to the OLT, the OLT automatically issues the RF parameter profile to the remote extended frames, without requiring any software configuration. **NOTE** After the cable initialization profile is configured, a remote extended frame uses the RF port parameters configured in the profile after going online, regardless of whether the remote extended frame in added in offline mode or automatically discovered by the OLT.	● If the RF port parameters are the same for all the remote extended frames to be deployed in batches, use the cable initialization profile to configure the parameters. ● If the RF port parameters are basically the same for all the remote extended frames to be deployed in batches, use the cable initialization profile to configure the parameters. Then modify parameter settings in customized cable configuration mode.
Customize RF port parameters in cable mode.	Requires differentiated plans and configurations for RF port parameters of remote extended frames and the remote extended frames must be configured one by one.	If the RF port parameters are greatly different for the remote extended frames to be deployed in batches, use this method to configure the parameters.

Copyright © Huawei Technologies Co., Ltd.

Data Plan

Table 15-56 Data plan for RF port parameters

Item	Data
RF port	1/1/0
Upstream channels	● IDs: 1-4 ● Type: European standard (default channel type) ● ID of the upstream channel modulation profile: 1 (by default) ● Channel central frequency (MHz): 29.8, 42.60, 49.00, and 55.4
Downstream channels	● IDs: 1-16 ● Type: European standard (default channel type) ● Channel central frequency (MHz): 602.00, 610.00, 618.00, ..., and 722.00

Procedure

- Use a cable initialization profile to configure RF port parameters.
  1. Configure the frequency spectrum range and channel type.

     In this example, the channel is of the European type. To change the type to North American, run the **cable** command.
  2. Configure RF port parameters for upstream channels and activate the upstream channels.

Parameter	Description
frequency and **channel-width**	A central frequency and a frequency bandwidth determine a frequency range, within which packets are transmitted. For example, the central frequency of a European channel is 55 MHz and the frequency bandwidth is 6400 kHz. Then the frequency range of the channel is 51.8-58.2 MHz.
modulation-profile	An upstream channel modulation profile defines parameters for processing the signals transmitted over the upstream channel. You do not need to configure an upstream channel modulation profile generally. Ports automatically bind to profile 1 by default.

The following configurations are used as an example to configure RF parameters for upstream channels:

Copyright © Huawei Technologies Co., Ltd.

- Number of upstream channels: 4
- Frequency bandwidth of the channels: 3.2 MHz (default value)

```
huawei(config)#interface cable init-template
huawei(config-cable-init-template)#cable upstream 1 frequency 29.8 enable
huawei(config-cable-init-template)#cable upstream 2 frequency 42.60
enable
huawei(config-cable-init-template)#cable upstream 3 frequency 49.00
enable
huawei(config-cable-init-template)#cable upstream 4 frequency 55.40
enable
```

3. Configure RF port parameters for downstream channels and activate the downstream channels.

Parameter	Description
modulation	A greater modulation mode value for downstream channels results in a higher channel bandwidth but weaker anti-interference capability. Therefore, configure the modulation mode based on site requirements. The default modulation mode is QAM256. This example uses the default setting.

The following configuration is used as an example to configure RF parameters for downstream channels: A total of 16 downstream channels have been purchased.

```
huawei(config-cable-init-template)#cable downstream 1 frequency 602.00
enable
huawei(config-cable-init-template)#cable downstream 2 frequency 610.00
enable
huawei(config-cable-init-template)#cable downstream 3 frequency 618.00
enable
huawei(config-cable-init-template)#cable downstream 4 frequency 626.00
enable
huawei(config-cable-init-template)#cable downstream 5 frequency 634.00
enable
huawei(config-cable-init-template)#cable downstream 6 frequency 642.00
enable
huawei(config-cable-init-template)#cable downstream 7 frequency 650.00
enable
huawei(config-cable-init-template)#cable downstream 8 frequency 658.00
enable
huawei(config-cable-init-template)#cable downstream 9 frequency 666.00
enable
huawei(config-cable-init-template)#cable downstream 10 frequency 674.00
enable
huawei(config-cable-init-template)#cable downstream 11 frequency 682.00
enable
huawei(config-cable-init-template)#cable downstream 12 frequency 690.00
enable
huawei(config-cable-init-template)#cable downstream 13 frequency 698.00
enable
huawei(config-cable-init-template)#cable downstream 14 frequency 706.00
enable
huawei(config-cable-init-template)#cable downstream 15 frequency 714.00
enable
```


Copyright © Huawei Technologies Co., Ltd.

```
huawei(config-cable-init-template)#cable downstream 16 frequency 722.00
enable
```

- Customize the RF port parameters in cable mode.

  NOTE

  The configuration is complete if you have configured the RF port parameters using a cable initialization profile. For details, see **Use a cable initialization profile to configure RF port parameters**. Perform this operation if you need to customize the RF port parameters of a remote extended frame.

  1. Configure RF port parameters for upstream channels and activate the upstream channels.

     ```
     huawei(config)#interface cable 1/1/0
     huawei(config-if-cable-1/1/0)#cable upstream 1 frequency 29.8 enable
     huawei(config-if-cable-1/1/0)#cable upstream 2 frequency 42.60 enable
     huawei(config-if-cable-1/1/0)#cable upstream 3 frequency 49.00 enable
     huawei(config-if-cable-1/1/0)#cable upstream 4 frequency 55.40 enable
     ```

  2. Configure RF port parameters for downstream channels and activate the downstream channels.

     ```
     huawei(config-if-cable-1/1/0)#cable downstream 1 frequency 602.00 enable
     huawei(config-if-cable-1/1/0)#cable downstream 2 frequency 610.00 enable
     huawei(config-if-cable-1/1/0)#cable downstream 3 frequency 618.00 enable
     huawei(config-if-cable-1/1/0)#cable downstream 4 frequency 626.00 enable
     huawei(config-if-cable-1/1/0)#cable downstream 5 frequency 634.00 enable
     huawei(config-if-cable-1/1/0)#cable downstream 6 frequency 642.00 enable
     huawei(config-if-cable-1/1/0)#cable downstream 7 frequency 650.00 enable
     huawei(config-if-cable-1/1/0)#cable downstream 8 frequency 658.00 enable
     huawei(config-if-cable-1/1/0)#cable downstream 9 frequency 666.00 enable
     huawei(config-if-cable-1/1/0)#cable downstream 10 frequency 674.00 enable
     huawei(config-if-cable-1/1/0)#cable downstream 11 frequency 682.00 enable
     huawei(config-if-cable-1/1/0)#cable downstream 12 frequency 690.00 enable
     huawei(config-if-cable-1/1/0)#cable downstream 13 frequency 698.00 enable
     huawei(config-if-cable-1/1/0)#cable downstream 14 frequency 706.00 enable
     huawei(config-if-cable-1/1/0)#cable downstream 15 frequency 714.00 enable
     huawei(config-if-cable-1/1/0)#cable downstream 16 frequency 722.00 enable
     ```

----End

Result

1. The transmit power of the downstream channels meets site requirements.

   Run the **display cable downstream** *frameid/slotid/portid* { **all** | *channel-id* } **status** command to check whether the RF port parameters meet site requirements.

2. The signal-to-noise (SNR) ratio of the upstream channels meets site requirements.

   Run the **display cable signal quality** [*frameid/slotid/portid* [**upstream** *channel-id*]] command to check whether the RF port parameters meet site requirements. A greater SNR ratio results in better signal quality. The recommended SNR ratio is greater than 30 dB.

15.5.1.5 Configuring the HSI Service

A CM connects to an MA5633 through a cable and provides the HSI service for users.

Copyright © Huawei Technologies Co., Ltd.

Data Plan

Table 15-57 Data plan for the HSI service

Item	Data
VLAN	Tag type of the packets sent by the PC: untagged; VLAN ID of the HGW management packets (HGW Mg) added on the HGW: 300; transmission mode of the HGW management packets on the HGW: transparent transmission VLAN ID of the HSI service packets and CM management packets (CM Mg) added on the MA5633: 100; type of the VLAN: smart; attribute of the VLAN: common Name of a cable service domain: huawei
Uplink port	Forwarding DHCP and broadband packets: 0/4/0 Forwarding CM and HGW management packets: 0/5/0

Procedure

Step 1 Create an S-VLAN.

```
huawei(config)#vlan 100 smart
huawei(config)#vlan 300 smart
huawei(config)#port vlan 100 0/4 0
huawei(config)#port vlan 100 0/5 0
huawei(config)#port vlan 300 0/5 0
```

Step 2 Create a CM S-VLAN.

```
huawei(config)#cable service-vlan 100
  Info: The new service VLAN will take effect after the CM is restarted, are you
 sure to modify? (y/n)[n]:y
```

Step 3 Add cable service domain **huawei**, add the HSI service to this service domain, and configure mapping rules.

```
huawei(config)#cable service-domain huawei
huawei(config-cable-srv-domain-huawei)#mapping vlan 100 tag-transform add if-match
user-vlan untagged
huawei(config-cable-srv-domain-huawei)#mapping vlan 300 tag-transform translate if-
match user-vlan 300    //Transparently transmitting HGW management packets
huawei(config-cable-srv-domain-huawei)#member cm ip-prefix 10.10.10.0 255.255.255.0
```

----End

15.5.1.6 Configuring the DOCSIS VoD Service

A CM connects to an MA5633 through a cable and provides the DOCSIS VoD service for users.

Copyright © Huawei Technologies Co., Ltd.

Data Plan

Table 15-58 Data plan for the DOCSIS VoD service

Item	Data
VLAN	Tag type of the packets sent by the STB: untagged; VLAN ID of the VoD packets added on the HGW: 200; type of the VLAN: smart; attribute of the VLAN: common Transmission mode of the VoD packets on the MA5633: transparent transmission Name of a cable service domain: huawei
Uplink port	Forwarding VoD packets: 0/5/0

Procedure

Step 1 Create an S-VLAN.

```
huawei(config)#vlan 200 smart
huawei(config)#port vlan 200 0/5 0
```

Step 2 Add cable service domain **huawei**, add the VoD service to this service domain, and configure mapping rules.

```
huawei(config)#cable service-domain huawei
huawei(config-cable-srv-domain-huawei)#mapping vlan 200 tag-transform translate if-match user-vlan 200    //Transparently transmitting VoD packets
huawei(config-cable-srv-domain-huawei)#member cm ip-prefix 10.10.10.0 255.255.255.0
```

----End

15.5.1.7 Verifying Services

A distributed cable modem termination system (D-CMTS) working as a remote extended frame locates on an optical node. To facilitate service verification, the optical line terminal (OLT) supports multiple remote service verification methods, such as Dynamic Host Configuration Protocol (DHCP) dialup emulation tests. This allows commissioning and configuration engineers to remotely verify services. In addition, this section describes how to verify the home services on site.

Prerequisites

- The OLT is properly connected to the upper-layer network.
- The DHCP server, Trivial File Transfer Protocol (TFTP) server, and softswitch or IP multimedia subsystem (IMS) have been configured.

Procedure

- Perform a DHCP dialup emulation test.

  In this test, a cable modem (CM) is emulated on the OLT to apply to the DHCP server for an IP address. This checks whether the OLT can communicate with the DHCP server and verifies CM DHCP configurations on the DHCP relay, proxy, and server.

Copyright © Huawei Technologies Co., Ltd.

1. Run the **simulate dhcp start cm** *mac-address* [**option60** *option60*] command to start a DHCP dialup emulation test.

   NOTE

   You can run the **simulate dhcp stop** command to stop the DHCP emulation.
2. Run the **display simulation dhcp** command to query the results of the DHCP dialup emulation test.
3. Check whether the **User IP** has obtained an IP address.

- Check the CM status.

  Run the **display cable modem** command to query the CM status in **Status**.

```
huawei(config)#display cable modem  all

------------------------------------------------------------------------------
-
 Idx    MAC            IP              I/F          Status   Prim  Num Ver  DS
RX
                                                             SID   CPE
Power

------------------------------------------------------------------------------
-
 1      0023-ED6F-21A3 192.168.1.118   1/1/0/U4     ol-pt    1     0    D2.0
-

------------------------------------------------------------------------------
-
 Total:
1
 ol: 0, ol-ptd: 0, ol-pt: 1, ol-d: 0, wol: 0, wol-ptd: 0, wol-pt: 0, wol-d:
0,
pol: 0, pol-ptd: 0, pol-pt: 0, pol-d: 0, offline: 0, rej-m: 0, rej-pt: 0, rej-
o:
 0, init: 0, init-rc: 0, DHCP: 0, DHCP-O: 0, DHCP-R: 0, DHCP-C: 0, REG:
0
 Note: 1. Idx is the index of a
CM.
       2. The downstream received power is in the unit of
dBmV.
       3. In status, "ol" means online, "rej" means reject.
```

  The following table lists the CM status and handling suggestions.

CM Status	Description	Handling Suggestion
init	Indicates that the CM initialization ranging message is received.the CM initialization.	If a CM is always in the ranging state, the ranging fails. Then check radio frequency (RF) line indicators and detect line faults.
init-rc	Indicates that the CM initialization ranging is complete.	No action is required. The ranging of the CM is complete.
DHCP	Indicates that the DHCP discovery from the CM is received.	If a CM initiates a DHCP request but does not obtain an IP address, check the DHCP server, routing between the OLT and the DHCP server, and DHCP server parameter settings.

Copyright © Huawei Technologies Co., Ltd.

CM Status	Description	Handling Suggestion
● DHCP-O ● DHCP-R ● DHCP-C	● DHCP-O: indicates that the offer from the DHCP server is received. ● DHCP-R: indicates that the DHCP request from the CM is received. ● DHCP-C: indicates that the acknowledge from the DHCP server is received.	The DHCP server has assigned an IP address to the CM and sent configuration file name and IP address of the TFTP or ToD server to the CM using the Option 67 and Option 66 fields (the Option 67 field carries the configuration file name and the Option 66 field carries the IP address of the TFTP or ToD server). If the CM is always in the DHCP-C state, the CM fails to obtain the configuration file. Then check the TFTP server, routing between the OLT and the TFTP server, and TFTP server parameter settings.
REG	Indicates that a registration is started.	If the CM is always in the register state, the CM obtains an incorrect configuration file. Then change the configuration file.

Copyright © Huawei Technologies Co., Ltd.

CM Status	Description	Handling Suggestion
● ol ● ol-pt ● ol-ptd ● ol-d ● wol ● wol-pt ● wol-ptd ● wol-d ● pol ● pol-pt ● pol-ptd	● ol: indicates that the CM is online. (valid only for CMs complying with DOCSIS 2.0) ● ol-pt: indicates that the CM is online and passes the BPI authentication. (valid only for CMs complying with DOCSIS 2.0) ● ol-ptd: indicates that the CM is online and passes the BPI authentication, and NetAccessEnable is disabled. (valid only for CMs complying with DOCSIS 2.0) ● ol-d: indicates that the CM is online and NetAccessEnable is disabled. (valid only for CMs complying with DOCSIS 2.0) ● wol: indicates that the CM is online and all channels bound to the CM are available. (valid only for CMs complying with DOCSIS 3.0) ● wol-pt: indicates that the CM is online and passes the BPI authentication, and all channels bound to the CM are available. (valid only for CMs complying with DOCSIS 3.0) ● wol-ptd: indicates that the CM is online and passes the BPI authentication, NetAccessEnable is disabled, and all channels bound to the CM are available. (valid only for CMs complying with DOCSIS 3.0) ● wol-d: indicates that the CM is online, NetAccessEnable is disabled, and all channels bound to the CM are available. (valid only for CMs complying with DOCSIS 3.0) ● pol: indicates that the CM is online and some channels	No action is required. The status indicates that the CM has registered

Copyright © Huawei Technologies Co., Ltd.

CM Status	Description	Handling Suggestion
● pol-d	bound to the CM are available. (valid only for CMs complying with DOCSIS 3.0) ● pol-pt: indicates that the CM is online and passes the BPI authentication, and some channels bound to the CM are available. (valid only for CMs complying with DOCSIS 3.0) ● pol-ptd: indicates that the CM is online and passes the BPI authentication, NetAccessEnable is disabled, and some channels bound to the CM are available. (valid only for CMs complying with DOCSIS 3.0) ● pol-d: indicates that the CM is online, NetAccessEnable is disabled, and some channels bound to the CM are available. (valid only for CMs complying with DOCSIS 3.0)	with the OLT and can correctly transmit and receive services.
offline	Indicates the offline status.	If the CM is in the offline state, check the power status, noise, and channel frequency of the CM.
● rej-m ● rej-pt ● rej-o	● rej-m: indicates that the MIC verification fails. ● rej-pt: indicates that the BPI authentication fails. ● rej-o: indicates that the authentication reject due to other reasons.	If the CM is in the reject state, no service flow can be created. Then check the CM authentication and CM message integrity check (MIC), and check whether class of service (COS) parameters specified in the CM configuration file are supported by the OLT.

- Verify that home services can be provisioned.
  1. After the CM is installed at a user home and commissioned, the user can watch TV programs.
  2. After the high-speed Internet (HSI) service is provisioned, the user can access the Internet from a PC.
  3. After the VoD service is provisioned, the user can order programs.

----End

Copyright © Huawei Technologies Co., Ltd.

16 OptiCable D-CMTS Configuration (MA5633 Working as a Standalone NE)

About This Chapter

The 0ptiCable solution implements cable TV (CATV) and broadband signal transmission over a coaxial network. It applies in CATV network reconstruction in upstream and downstream directions or new residential areas requiring the CATV and broadband services over a coaxial network. The radio frequency (RF) access mode applies in the PON+distributed cable modem termination system (D-CMTS) scenario or GE+D-CMTS scenario. This mode complies with the data over cable service interface specification (DOCSIS) and supports multiple broadcast and TV services, such as high-speed Internet (HSI) and IPTV services.

16.1 D-CMTS Service Overview
This section describes the services supported by a distributed cable modem termination system (D-CMTS) for multiservice operators (MSOs) from the aspect of basic concepts, networking scenarios, and hardware configurations. This information provides a basis for configuring the services on the D-CMTS.

16.2 Data Plan Principles for D-CMTS Services
This section describes the principles of planning frequency spectrum management, device management, quality of service (QoS), and VLANs for distributed cable modem termination system (D-CMTS) services.

16.3 Service Configuration on a D-CMTS That Works in GE Access Mode on a Layer 3 Network
This section describes how to configure services, including home services, L2VPN enterprise service, and wireless local area network (WLAN) hotspot radio backhaul service, on a distributed cable modem termination system (D-CMTS) that works in GE access mode on a Layer 3 network. The MA5603T equipped with the SCUV, OPGE, and SPUF boards is used as an example.

16.4 Service Configuration on a D-CMTS That Works in GPON Access Mode on a Layer 3 Network
This section describes how to configure services, including home services, L2VPN enterprise service, and wireless local area network (WLAN) hotspot radio backhaul service, on a distributed cable modem termination system (D-CMTS) that works in GPON access mode on a Layer 3

Copyright © Huawei Technologies Co., Ltd.

network. The MA5603T equipped with the SCUV, GPBH, and SPUF boards is used as an example.

Copyright © Huawei Technologies Co., Ltd.

16.1 D-CMTS Service Overview

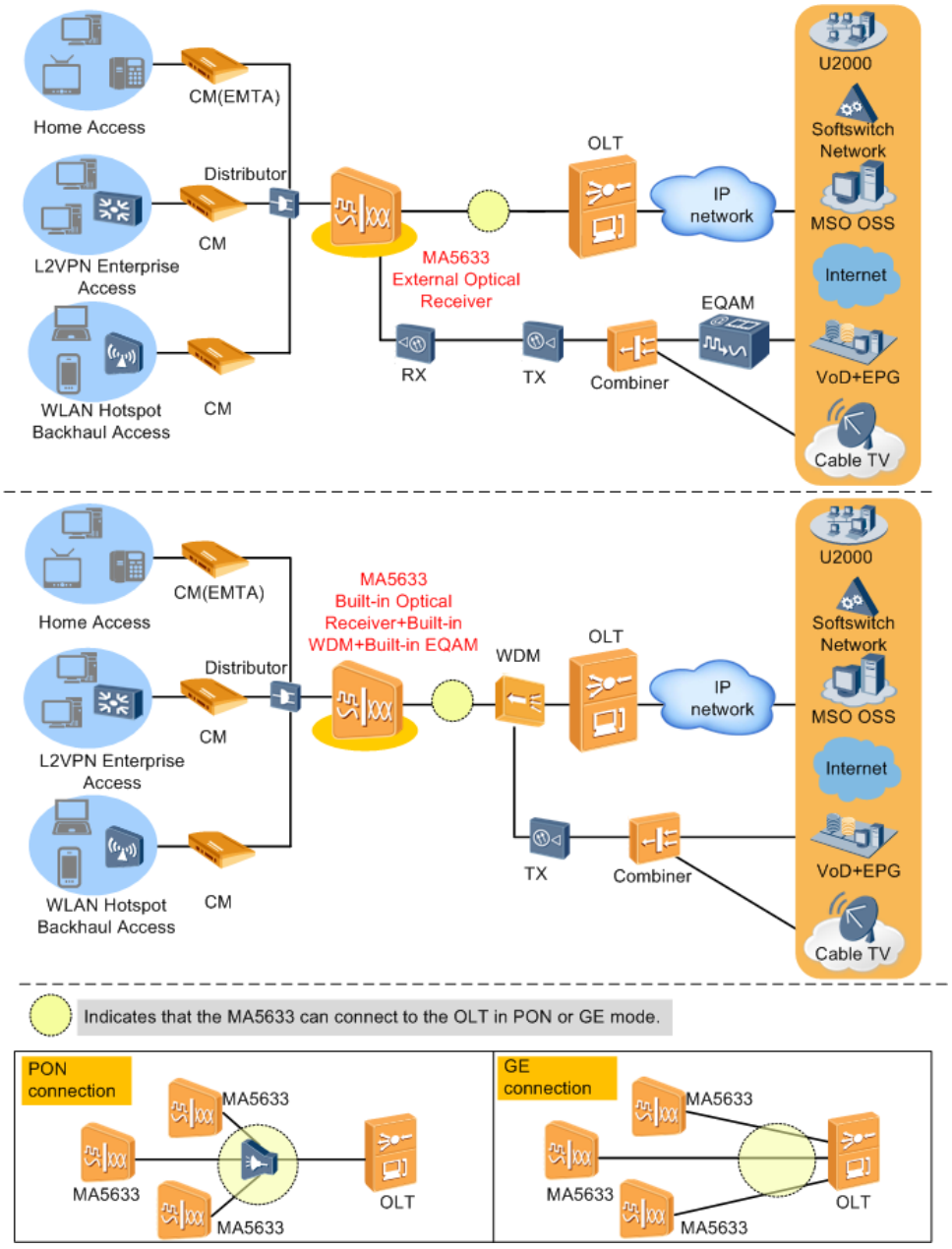
This section describes the services supported by a distributed cable modem termination system (D-CMTS) for multiservice operators (MSOs) from the aspect of basic concepts, networking scenarios, and hardware configurations. This information provides a basis for configuring the services on the D-CMTS.

16.1.1 Basic Concepts

This section describes basic concepts related to a distributed cable modem termination system (D-CMTS) from the user side to the network side on D-CMTS networks using PON and GE upstream transmission.

Copyright © Huawei Technologies Co., Ltd.

Figure 16-1 D-CMTS networking



User Home Side

Concept	Description
Cable modem (CM)	A device that connects customer premises equipment (CPE) to a hybrid fiber coaxial (HFC) network. It transmits data over a cable network through data over cable service interface specification (DOCSIS).

Copyright © Huawei Technologies Co., Ltd.

Concept	Description
Media terminal adapter (MTA)	A network client that provides user terminal (such as a phone set)-oriented ports and call control unit-oriented network signaling interfaces. It connects to cable network units through an HFC network. MTAs are classified into embedded MTAs (EMTAs) and single MTAs (SMTAs) according to PacketCable. ● An EMTA integrates CM and MTA functions. ● An SMTA supports only MTA functionalities.
VoD	A technology that enables users to order any program in a VoD program library. During program playing, users can perform operations, such as pause, fast forward, fast rewind, and program locating.
Distributor	A component that distributes signals in a cable TV (CATV) transmission system. It equally outputs several channels of signals from one channel of input signals. The common distribution ratios are 1:2, 1:3, 1:4, and 1:6.

Optical Node

Concept	Description
D-CMTS	A device that connects an aggregation network to an HFC network. It forwards network data, processes protocols, and modulates or demodulates radio frequency (RF) signals. The D-CMTS provides the quality of service (QoS) required by CMs and allocates upstream bandwidths and service resources to the CMs based on CMs' request and network QoS policy.
Built-in optical receiver	● An optical receiver, which performs optical-to-electrical (O/E) conversion for CATV and upstream backhaul signals. ● The fiber node does not require an additional optical receiver. The O/E conversion is performed by the optical receiver built in the MA5633 and the MA5633 can receive CATV optical signals.
Built-in WDM	● A device that multiplexes the optical signals with different standard wavelengths into one channel of multiplexed signals and transmits the signals over one optical fiber. ● The WDM in the branch equipment room combines data signals and CATV signals for signal transmission over one feeder fiber. On the optical node, the WDM built in the MA5633 separates the two types of signals from each other.

Copyright © Huawei Technologies Co., Ltd.

Concept	Description
Built-in EQAM	● The edge quadrature amplitude modulation (EQAM) feature enables the MA5633 to function as the gateway of a hybrid fiber coaxial (HFC) network connected to an IP network. The MA5633 multiplexes and modulates IP signals into radio frequency (RF) signals so that the data carried in the IP signals can be transmitted over the HFC network. ● The EQAM built in the MA5633 is moved downwards from the branch equipment room to the fiber node. Therefore, the fiber node does not require an additional EQAM. ● Video streams are transmitted over a MAN network through the OLT to the MA5633. The MA5633 uses the built-in EQAM to module the video signals into RF signals and sends the RF signals to the STB.
Splitter	A component that connects to the center of a branch or feeder fiber. It consists of a main input end, a main output end, and multiple branch output ends. Each branch output end receives only few input signals on the main path. The majority signals are transmitted forward over the main path.

Branch Equipment Room

Concept	Description
PON	A passive optical network (PON) uses a point-to-multipoint (P2MP) network architecture. A PON network consists of three parts: optical line terminal (OLT), optical distribution network (ODN), and optical network units (ONUs). A PON network uses optical fibers for data transmission, supports more users with less optical fiber resources, and provides a higher access rate. Mainstream PON technologies include broadband passive optical network (BPON), Ethernet passive optical network (EPON), and gigabit passive optical network (GPON).
Optical distribution network (ODN)	The ODN is composed of passive optical components, such as optical fibers and one or more passive optical splitters. The ODN provides highly reliable optical channels between the OLT and ONUs.
Optical line terminal (OLT)	The OLT is an aggregation device located at the central office (CO), which terminates PON protocols. OLTs in this document are MA5600T/MA5603T/MA5608T.
Optical splitter	A passive component, which allocates optical power to multiple ONUs connected to one feeder fiber. In a GPON network that consists of an OLT, ONUs, optical splitters, and optical fibers, the optical fiber connected to the OLT uses an optical splitter to connect to multiple ONUs. The number of ONUs that can be connected to the optical fiber is determined based on the split ratio.

Copyright © Huawei Technologies Co., Ltd.

Concept	Description
RX	An optical receiver, which performs optical-to-electrical (O/E) conversion for CATV and upstream backhaul signals.
TX	An optical transmitter, which performs O/E conversion for received CATV signals.
Combiner	A component that combines multiple channels of analog signals into one channel of signals on an RF port and then sends the signals to the downstream optical TX.

MAN Network

Concept	Description
Softswitch or IP multimedia subsystem (IMS)	Softswitch: core of the NGN network call and control, which supports call and connection control for the services having high real-time requirements. For the softswitch, services are separated from call control and call control is separated from bearing. In addition, the softswitch uses open service interface (API) and standard protocols, which facilitates the development for new services and features. IMS: uses Session Initiation Protocol (SIP) signaling as the call control signaling. It provides voice, data, and multimedia services.
Broadband TV (BTV) source	IPTV head end, a contents preparation platform in the IPTV system. It receives signals, converts media formats, and manages media materials.

16.1.2 Networking Scenarios and Hardware Configurations

This section describes networking scenarios of a distributed cable modem termination system (D-CMTS) and D-CMTS's hardware configurations.

Copyright © Huawei Technologies Co., Ltd.

Networking Scenarios and Hardware Configurations

Networking Scenario	Description	OLT Device	ONU Device
Home service networking	In home service networking, an MA5633 connects to cable modems (CMs) at user homes through radio frequency (RF) ports and provides home services for users, including the cable TV (CATV) service, Internet access service, VoD service, broadband TV (BTV) service, and PacketCable service.	● MA5603T/ MA5600T: SCUV+GPMD +SPUF or SCUV+OPGE/ ETHB+SPUF ● MA5608T: MCUE+GPMD +SPUF or MCUE+OPGE/ ETHB+SPUF	● Equipped with a built-in optical receiver: MA5633, providing 4-out radio frequency (RF) ports ● Equipped without a built-in optical receiver: MA5633, providing 2-in-2-out or 4-in-4-out RF ports ● Equipped with a built-in WDM: MA5633, providing 4-out radio frequency (RF) ports
L2VPN enterprise service networking	In L2VPN enterprise service networking, an MA5633 connects to cable modems (CMs) through radio frequency (RF) ports, and the CMs connect to switches to provide the L2VPN service for users.		
Wireless local area network (WLAN) hotspot radio backhaul service networking	In wireless local area network (WLAN) hotspot radio backhaul service networking, an MA5633 connects to cable modems (CMs) through radio frequency (RF) ports. A CM connects to wireless access points (APs) to provide wireless fidelity (Wi-Fi) access for users.		

16.2 Data Plan Principles for D-CMTS Services

This section describes the principles of planning frequency spectrum management, device management, quality of service (QoS), and VLANs for distributed cable modem termination system (D-CMTS) services.

16.2.1 Frequency Spectrum Management

Copyright © Huawei Technologies Co., Ltd.

Total Frequency Bandwidth

The total frequency bandwidth supported by a distributed cable modem termination system (D-CMTS) ranges from 5 MHz to 1 GHz.

Upstream Frequency Bandwidth

The upstream frequency bandwidth supported by a D-CMTS can be of the European or North American standard.

- European standard: 5 MHz to 65 MHz
- North American standard: 5 MHz to 42 MHz

Downstream Frequency Bandwidth

The downstream frequency bandwidth supported by a D-CMTS can be of the European or North American standard.

- European standard: 87 MHz to 1002 MHz
- North American standard: 57 MHz to 1002 MHz

Recommended Frequency Spectrum Configuration

Figure 16-2 lists the recommended frequency spectrum configuration, using the European standard as an example.

Figure 16-2 Recommended frequency spectrum configuration

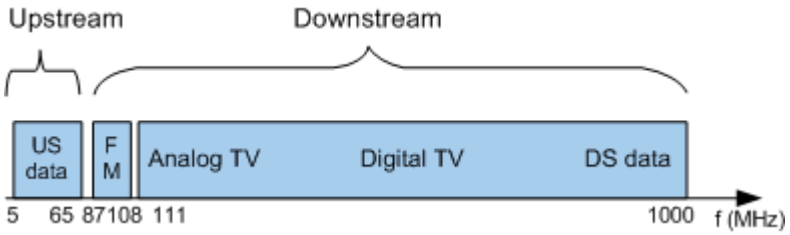


Table 16-1 Description of recommended frequency spectrum configuration

Item	Planning Suggestion	Planning Principle
Upstream frequency bandwidth	The upstream frequency bandwidth ranging from 5 MHz to 15 MHz is used to transmit low-traffic data without strict requirements on signal-to-noise ratio (SNR), such as network status monitoring, VoD, user passwords, and program indexes.	● Plan the upstream frequency bandwidth for the cable TV (CATV) service to support the services that have been provisioned and those to be provisioned. ● Plan continuous upstream frequency bandwidths for the analog TV service, digital TV service, and data over cable service interface specification (DOCSIS) data service to prevent interference between the services. In addition, the planning should facilitate
	The upstream frequency bandwidth ranging from 16 MHz to 65 MHz is used to transmit upstream data.	

Copyright © Huawei Technologies Co., Ltd.

Item	Planning Suggestion	Planning Principle
Downstream frequency bandwidth	The downstream frequency bandwidth ranging from 87 MHz to 108 MHz is used to carry the frequency modulation (FM) broadcast service. The FM frequency is 400 kHz. The downstream frequency bandwidth supports 52 frequency points.	the system in handling the issues of a service without affecting other services.
	The downstream frequency bandwidth ranging from 111 MHz to 1 GHz is used to carry the analog TV service, digital service, and DOCSIS data service. In the range from 111 MHz to 1 GHz: ● 111 MHz to 550 MHz: analog TV service ● 550 MHz to 750 MHz: digital TV service ● 750 MHz to 1 GHz: DOCSIS data service	

16.2.2 Device Management

Data Plan for Device Management

Item	Device or Service	Planning Principle
Management channel	Optical line terminal (OLT)	The management VLANs of all OLTs on an entire network carry only service VLAN tags.
	MA5633	The management VLANs of all MA5633s on an entire network carry only VLAN tags.
IP address	Device management	The management IP address of an OLT uses a private IP address to ensure the OLT security.
	Cable modem (CM)	A CM obtains a private IP address through Dynamic Host Configuration Protocol (DHCP).
	Internet access service	The high-speed Internet (HSI) service uses public IP addresses, which are planned by carriers.
	PacketCable service	A media terminal adapter (MTA) obtains a private IP address through DHCP.

Copyright © Huawei Technologies Co., Ltd.

Item	Device or Service	Planning Principle
	VoD and broadband TV (BTV) services	A set top box (STB) obtains a private IP address through DHCP for program ordering.

16.2.3 QoS

Quality of service (QoS) planning varies according to service types. For details, see **Table 15-2**.

Service Priority Planning and Queue Scheduling Policy

Table 16-2 Service priority planning and queue scheduling policy

Service Type	802.1p	Queue
Network protocol and signaling	6	CS6 (PQ)
VoIP	5	EF (PQ)
IPTV, OAM for EMS or NMS, and golden enterprises	4	AF4 (WFQ)
Silver enterprise	3	AF3 (WFQ)
Bronze enterprise	2	AF2 (WFQ)
High-speed Internet (HSI) service	0	BE (WFQ)

NOTE

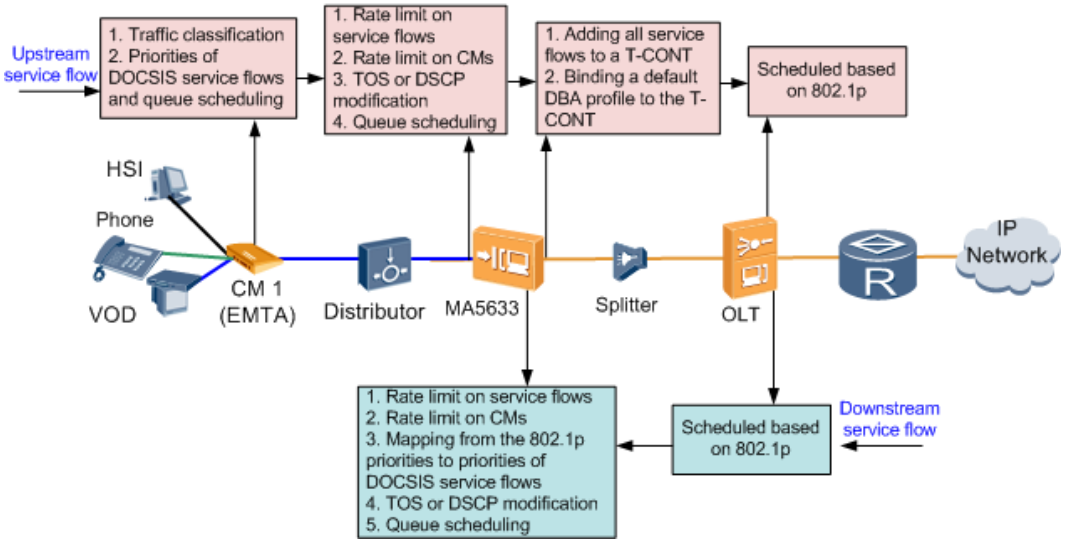
The priorities listed in the preceding table are recommended. Change the priorities based on site and carriers' requirements.

QoS Model

Figure 16-3 shows the end to end (E2E) QoS processing for the data over cable service interface specification (DOCSIS) service.

Copyright © Huawei Technologies Co., Ltd.

Figure 16-3 QoS model for a D-CMTS



Copyright © Huawei Technologies Co., Ltd.

Table 16-3 QoS planning principles

Service	Packet Direction	QoS Planning		
		CM or Switch	D-CMTS	OLT
Cable modem (CM) control service, HSI service, or VoIP service	Upstream	1. A CM classifies flows for service packets. 2. A CM schedules queues according to the priorities of DOCSIS service flows.	QoS parameters are defined in a CM configuration file. Using the QoS parameter settings, a D-CMTS limits service rates or schedules queues by priorities. In addition, an OLT supports the configuration of a QoS profile, which defines QoS parameters for various CM services. If a QoS parameter is defined both in a CM configuration file and a QoS profile, the configuration in the CM configuration file preferentially takes effect. 1. A D-CMTS limits CM service rates based on service priority. 2. A D-CMTS limits the rate of a CM service flow group. 3. A D-CMTS schedules queues for service flows. GPON module 1. All service flows are mapped from GPON encapsulation mode (GEM) port 0 to transmission container (T-CONT) 1. 2. T-CONT 1 is bound to the default	An OLT maps the priority of a DOCSIS service flow to the 802.1p field in the Ethernet header and uses the 802.1p priority to schedule queues.

Copyright © Huawei Technologies Co., Ltd.

Service	Packet Direction	QoS Planning		
		CM or Switch	D-CMTS	OLT
			dynamic bandwidth allocation (DBA) profile. T-CONT 1 is of type 4 and supports a maximum bandwidth of 1000 Mbit/s.	
	Downstream	A CM does not control traffic.	A D-CMTS controls traffic based on traffic settings of DOCSIS service flows and performs committed access rate (CAR) based on the CM traffic control parameters defined in a CM configuration file.	An OLT uses the 802.1p priority to schedule queues.
L2VPN enterprise or wireless local area network (WLAN) hotspot radio backhaul service	The QoS processing for L2VPN enterprise and WLAN hotspot radio backhaul services is the same as that for home services.			

16.2.4 VLAN

Copyright © Huawei Technologies Co., Ltd.

Table 16-4 VLAN planning principles

Service	VLAN Tag Translation			
	CM	**D-CMTS**	**OLT**	**Layer 3 MAN Device**
Internet access service	The packets of the Internet access service do not carry a VLAN tag. A service flow is created between a cable modem (CM) and a distributed cable modem termination system (D-CMTS).	CM management packets and high-speed Internet (HSI) packets carry the same VLAN tag.	● When an optical line terminal (OLT) forwards services at Layer 2, the OLT transparently transmits VLAN tags to a metropolitan area network (MAN) device. ● When an OLT forwards services at Layer 3, the OLT adds a unique VLAN tag to the packets of a service type.	● When an OLT forwards services at Layer 2, a Layer 3 MAN device forwards the services at Layer 3 and adds a unique VLAN tag to the packets of a service type. ● When an OLT forwards services at Layer 3, a Layer 3 MAN device forwards the services at Layer 3.
VoD service	The packets of the VoD service do not carry a VLAN tag. A service flow is created between a CM and a D-CMTS.	CM management packets and electronic program guide (EPG) packets carry the same VLAN tag.	● When an OLT forwards services at Layer 2, the OLT transparently transmits VLAN tags to a MAN device. ● When an OLT forwards services at Layer 3, the OLT adds a unique VLAN tag to the packets of a service type.	● When an OLT forwards services at Layer 2, a Layer 3 MAN device forwards the services at Layer 3 and adds a unique VLAN tag to the packets of a service type. ● When an OLT forwards services at Layer 3, a Layer 3 MAN device forwards the services at Layer 3.

Copyright © Huawei Technologies Co., Ltd.

Service	VLAN Tag Translation			
	CM	D-CMTS	OLT	Layer 3 MAN Device
Multicast service	The packets of the multicast service do not carry a VLAN tag. A service flow is created between a CM and a D-CMTS.	CM management packets and multicast packets carry the same VLAN tag.	● When an OLT forwards services at Layer 2, the OLT transparently transmits VLAN tags to a MAN device. ● When an OLT forwards services at Layer 3, the OLT adds a unique VLAN tag to the packets of a service type.	● When an OLT forwards services at Layer 2, a Layer 3 MAN device forwards the services at Layer 3 and adds a unique VLAN tag to the packets of a service type. ● When an OLT forwards services at Layer 3, a Layer 3 MAN device forwards the services at Layer 3.
VoIP service	The packets of the VoIP service do not carry a VLAN tag. A service flow is created between a CM and a D-CMTS.	CM management packets and VoIP packets carry the same VLAN tag.	● When an OLT forwards services at Layer 2, the OLT transparently transmits VLAN tags to a MAN device. ● When an OLT forwards services at Layer 3, the OLT adds a unique VLAN tag to the packets of a service type.	● When an OLT forwards services at Layer 2, a Layer 3 MAN device forwards the services at Layer 3 and adds a unique VLAN tag to the packets of a service type. ● When an OLT forwards services at Layer 3, a Layer 3 MAN device forwards the services at Layer 3.

Copyright © Huawei Technologies Co., Ltd.

Service	VLAN Tag Translation			
	CM	D-CMTS	OLT	Layer 3 MAN Device
L2VPN enterprise service	Two service flows are created between a CM and a D-CMTS. One is the default service flow and the other is the VPN service flow.	CM management packets and enterprise packets carry different VLAN tags. The VLAN pre-configured for the packets of the L2VPN enterprise service must be the same as that configured in the CM configuration file if the L2VPN enterprise service is configured through a CM configuration file.	● When an OLT forwards services at Layer 2, the OLT transparently transmits VLAN tags to a MAN device. ● When an OLT forwards services at Layer 3, the OLT adds a unique VLAN tag to the packets of a service type.	● When an OLT forwards services at Layer 2, a Layer 3 MAN device forwards the services at Layer 3 and adds a unique VLAN tag to the packets of a service type. ● When an OLT forwards services at Layer 3, a Layer 3 MAN device forwards the services at Layer 3.
Wireless local area network (WLAN) hotspot radio backhaul service	The packets of the WLAN hotspot radio backhaul service do not carry a VLAN tag. Two service flows are created between a CM and a D-CMTS. One is the default service flow and the other is the wireless fidelity (Wi-Fi) service flow.	CM management packets and Wi-Fi packets carry different VLAN tags. The VLAN pre-configured for the Wi-Fi packets must be the same as that configured in the CM configuration file.	● When an OLT forwards services at Layer 2, the OLT transparently transmits VLAN tags to a MAN device. ● When an OLT forwards services at Layer 3, the OLT adds a unique VLAN tag to the packets of a service type.	● When an OLT forwards services at Layer 2, a Layer 3 MAN device forwards the services at Layer 3 and adds a unique VLAN tag to the packets of a service type. ● When an OLT forwards services at Layer 3, a Layer 3 MAN device forwards the services at Layer 3.

The VLAN planning principles are summarized as follows:

Copyright © Huawei Technologies Co., Ltd.

- HSI, VoIP, and CM management services for home users carry the same S-VLAN tag on a layer 3 network.
- HSI, VoIP, and CM management services for home users carry the different S-VLAN tags on a layer 2 telecom network. Service types can be identified based on VLANs.
- A D-CMTS identifies the L2VPN enterprise and WLAN hotspot radio backhaul services by S-VLAN tag.

16.3 Service Configuration on a D-CMTS That Works in GE Access Mode on a Layer 3 Network

This section describes how to configure services, including home services, L2VPN enterprise service, and wireless local area network (WLAN) hotspot radio backhaul service, on a distributed cable modem termination system (D-CMTS) that works in GE access mode on a Layer 3 network. The MA5603T equipped with the SCUV, OPGE, and SPUF boards is used as an example.

Control Board	SCUV
Interface Board	OPGE: 0/3
SPU Board	SPUF: 0/4, 0/5

NOTE

When an OPGE board is used, run the **network-role** command on the OLT to configure the ports on the OPGE board as cascading ports.

16.3.1 Home Service Networking

In home service networking, an MA5633 connects to cable modems (CMs) at user homes through radio frequency (RF) ports and provides home services for users, including the cable TV (CATV) service, Internet access service, VoD service, broadband TV (BTV) service, and PacketCable service. This section describes how to configure the optical line terminal (OLT) and the MA5633 to provision the home services.

NOTE

Configuration procedures are the same for IPv6 and IPv4 networks except in "Configure Dynamic Host Configuration Protocol (DHCP) relay" and "Configure a route". In addition, IPv6 does not support the function of configuring PacketCable dynamic voice services.

16.3.1.1 Service Requirements and Usage Scenario

Service Requirements

Users require the provisioning of the TV service, Internet access service, VoD service, broadband TV (BTV) service, and VoIP service. The TV service can be provisioned immediately after the distributed cable modem termination system (D-CMTS) hardware is connected. This section only describes how to configure the Internet access service, VoD service, BTV service, and VoIP service.

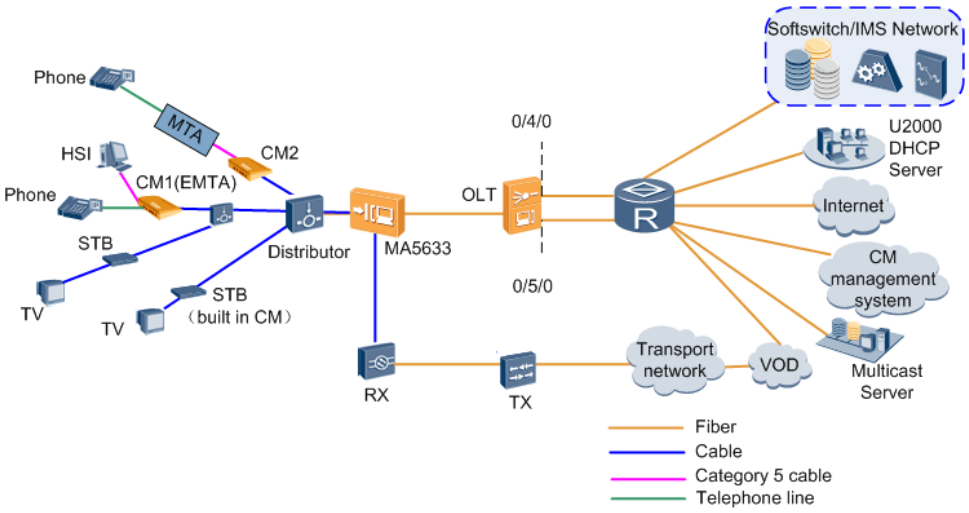
Copyright © Huawei Technologies Co., Ltd.

Usage Scenario

As shown in **Figure 16-4**, an MA5633 is deployed on an optical node and cable modems (CMs) are deployed at user homes. The CMs connect to radio frequency (RF) ports on the MA5633 through cables.

- Port 1 on CM 1 connects to a PC for the Internet access service, port 2 connects to a phone set for the VoIP service, and the distributor connects to the STB for the VoD service. CM 1 supports embedded media terminal adapter (EMTA) functions and the voice users of CM 1 use PacketCable 1.x.
- CM 2 does not support EMTA functions and needs to connect to a media terminal adapter (MTA). The voice users of CM 2 use PacketCable Multimedia.
- Users access the Internet through Dynamic Host Configuration Protocol (DHCP) dialup.
- The IP addresses of the CM, STB, PC, and MTA are assigned by the DHCP server and in different network segments.

Figure 16-4 Home service networking

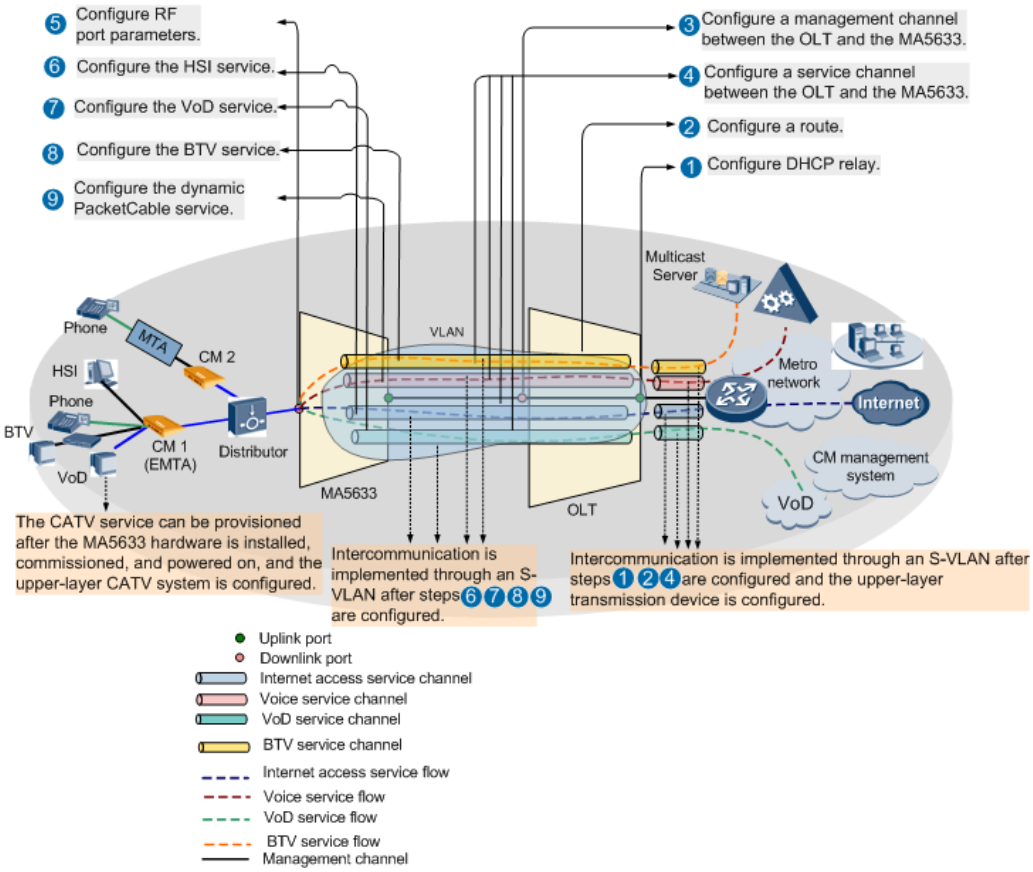


16.3.1.2 Configuration Process

Figure 16-5 shows the configuration roadmap for the home service networking.

Copyright © Huawei Technologies Co., Ltd.

Figure 16-5 Configuration roadmap for the home service networking



NOTE

Before logging in to the MA5633 to configure services on it, ensure that the MA5633 has been properly connected.

The following table describes the configuration steps.

Configuration Object	Step	Description
OLT	● IPv4: **Configure Dynamic Host Configuration Protocol (DHCP) relay.** ● IPv6: **Configure Dynamic Host Configuration Protocol (DHCP) relay (IPv6).**	This section describes how to configure Dynamic Host Configuration Protocol (DHCP) relay so that cable modems (CMs) can obtain IP addresses in different network segments.
	● IPv4: **Configure a route.** ● IPv6: **Configure a route (IPv6).**	This section describes how to implement network communication by configuring a route in Layer 3 networking with an optical line terminal (OLT). Through the route, packets are forwarded at Layer 3 between the OLT and its upper-layer devices or servers.

Copyright © Huawei Technologies Co., Ltd.

Configuration Object	Step	Description
	Configure a management channel between the OLT and the D-CMTS.	This section describes how to configure a management channel between an optical line terminal (OLT) and a distributed cable modem termination system (D-CMTS). After the configuration, you can log in to the D-CMTS from the OLT and configure the D-CMTS.
	Configure a service channel between the OLT and the D-CMTS.	This section describes how to configure a service channel between an optical line terminal (OLT) and a distributed cable modem termination system (D-CMTS). After the configuration, the service channel forwards service packets on the D-CMTS based on the planned VLAN and forwarding policy.
MA5633	**Configure radio frequency (RF) port parameters.**	Radio frequency (RF) port parameters define the frequency spectrum range for signal transmission and modulation mode. The configuration of RF port parameters implements data service transmission over cables.
	Configure the high-speed Internet (HSI) service.	None
	Configure the VoD service.	None
	Configure the broadband TV (BTV) service.	None
	Configure the dynamic PacketCable service.	None
	Verify the configured services.	An OLT supports multiple remote service verification methods. This allows commissioning and configuration engineers to remotely verify services. 1. A DHCP dialup emulation test checks whether the OLT can communicate with the DHCP server and verifies CM DHCP configurations on the DHCP relay, proxy, and server. 2. The status of a CM can be queried. Based on the information, you can determine whether the CM is online.

Copyright © Huawei Technologies Co., Ltd.

16.3.1.3 Configuring DHCP Relay

This section describes how to configure Dynamic Host Configuration Protocol (DHCP) relay so that cable modems (CMs) can obtain IP addresses in different network segments.

Prerequisites

The upper-layer router, DHCP server, and Trivial File Transfer Protocol (TFTP) server of an optical line terminal (OLT) have been configured.

Data Plan

Table 16-5 DHCP data plan for the OLT

Item	Data
VLAN	ID of the CM management S-VLAN: 100; type of the VLAN: smart
DHCP server group parameters	● IP address of the DHCP domain gateway for CMs: 10.10.224.1; domain name: docsis ● IP address of the DHCP domain gateway for media terminal adapters (MTAs): 10.100.224.1; domain name: pktc ● IP address of the DHCP domain gateway for paid PCs: 10.100.187.1; domain name: default ● IP address of the DHCP domain gateway for overdue PCs: 10.100.8.1; domain name: default ● IP address of the DHCP domain gateway for set top boxes (STB): 10.200.160.1; domain name: stb

Table 16-6 Data plan for the upper-layer devices of the OLT

Item	IP Address
Layer 3 interfaces connecting the router to the OLT	● Forwarding DHCP and broadband packets: 11.11.11.11 ● Forwarding CM management, VoD, and multicast packets: 11.11.12.11
IP addresses of DHCP servers	● DHCP server assigning IP addresses to CMs and MTAs: 192.168.10.10-192.168.10.11 ● DHCP server assigning IP addresses to PCs and STBs: 192.168.10.12-192.168.10.13
IP address of the TFTP server	192.168.5.10-192.168.5.13

Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Set the IP addresses of Layer 3 VLAN interfaces.

```
huawei(config)#vlan 100 smart
huawei(config)#interface vlanif 100
huawei(config-if-vlanif100)#arp proxy enable
huawei(config-if-vlanif100)#ip address 10.10.224.1 255.255.255.0 description
docsis     //Set the IP address of the DHCP domain gateway for CMs.
huawei(config-if-vlanif100)#ip address 10.100.224.1 255.255.255.0 sub description
pktc     //Set the IP address of the DHCP domain gateway for MTAs.
huawei(config-if-vlanif100)#ip address 10.200.160.1 255.255.255.0 sub description
stb     //Set the IP address of the DHCP domain gateway for STBs.
huawei(config-if-vlanif100)#ip address 10.100.187.1 255.255.255.0 sub description
default     //Set the IP address of the DHCP domain gateway for paid PCs.
huawei(config-if-vlanif100)#ip address 10.100.8.1 255.255.255.0 sub description
default      //Set the IP address of the DHCP domain gateway for overdue PCs.
huawei(config-if-vlanif100)#quit
```

Step 2 Configure the working mode of the DHCP relay to Layer 3 Option 60.

In DHCP Option 60 mode, a DHCP server group is selected according to the Option 60 domain name in DHCP packets. Users in this mode are identified by domain information of packets, which differentiates various service types in a VLAN. Ensure that the Option 60 domain name and the DHCP server group bound to the Option 60 domain name are configured beforehand.

```
huawei(config)#dhcp mode layer-3 Option60
  Several minutes may be required and no action can be taken during this period
  Are you sure to perform this operation? (y/n)[n]: y
```

Step 3 Enable the DHCP option82 feature.

The DHCP feature does not have any mechanism for authentication or security. Thus, the DHCP feature encounters many security problems when it is used in the network. To solve these problems, the DHCP option82 is introduced.

```
huawei(config)#dhcp option82 enable
```

Step 4 Set the IP addresses of the servers in a DHCP server group.

```
huawei(config)#dhcp-server 0 ip 192.168.10.10 192.168.10.11    //Configure DHCP
server group 0 to assign IP addresses to CMs and MTAs.
huawei(config)#dhcp-server 1 ip 192.168.10.12 192.168.10.13    //Configure DHCP
server group 1 to assign IP addresses to PCs and STBs.
```

Step 5 Create a DHCP Option 60 domain.

```
huawei(config)#dhcp domain default   //Create Option 60 domain name default for
PCs.
huawei(config-dhcp-domain-default)#dhcp-gateway learning enable   //Paid and
overdue PCs are in different network segments. Therefore, self-learning needs to be
enabled on OLT gateways.
huawei(config-dhcp-domain-default)#dhcp-server 1 vlan 100       //Bind DHCP server
group 1 to the DHCP domain where the PCs locate. After the configuration, the PCs
in the DHCP domain are corresponded to DHCP server group 1.
huawei(config-dhcp-domain-default)#quit
huawei(config)#dhcp domain docsis   //Create Option 60 domain name docsis for CMs.
huawei(config-dhcp-domain-docsis)#dhcp-server 0 vlan 100       //Bind DHCP server
group 0 to the DHCP domain where the CMs locate. After the configuration, the CMs
in the DHCP domain are corresponded to DHCP server group 0.
huawei(config-dhcp-domain-docsis)#quit
huawei(config)#dhcp domain pktc   //Create Option 60 domain name pktc for MTAs.
huawei(config-dhcp-domain-pktc)#dhcp-server 0 vlan 100       //Bind DHCP server
group 0 to the DHCP domain where the MTAs locate. After the configuration, the CMs
in the DHCP domain are corresponded to DHCP server group 0.
huawei(config-dhcp-domain-pktc)#quit
```


Copyright © Huawei Technologies Co., Ltd.

```
huawei(config)#dhcp domain stb   //Create Option 60 domain name stb for STBs.
huawei(config-dhcp-domain-stb)#dhcp-server 1 vlan 100     //Bind DHCP server group
1 to the DHCP domain where the STBs locate. After the configuration, the STBs in
the DHCP domain are corresponded to DHCP server group 1.
huawei(config-dhcp-domain-stb)#quit
```

Step 6 Set IP addresses of the gateways for the DHCP domain.

```
huawei(config)#interface vlanif 100
huawei(config-if-vlanif100)#dhcp domain default gateway 10.100.187.1
10.100.8.1    //Set the IP address of the gateway for the PC domain to 10.100.187.1
for paid PCs and to 10.100.8.1 for overdue PCs.
huawei(config-if-vlanif100)#dhcp domain docsis gateway 10.10.224.1    //Set the IP
address of the gateway for the CM domain to 10.10.224.1.
huawei(config-if-vlanif100)#dhcp domain pktc gateway 10.100.224.1    //Set the IP
address of the gateway for the MTA domain to 10.100.224.1.
huawei(config-if-vlanif100)#dhcp domain stb gateway 10.200.160.1    //Set the IP
address of the gateway for the STB domain to 10.200.160.1.
huawei(config-if-vlanif100)#quit
```

----End

16.3.1.4 Configuring a Route

This section describes how to implement network communication by configuring a route in Layer 3 networking with an optical line terminal (OLT). Through the route, packets are forwarded at Layer 3 between the OLT and its upper-layer devices or servers.

Prerequisites

The upper-layer router has been configured.

Data Plan

Table 16-7 Data plan for the Layer 3 interfaces on the network side

Item	IP Address
Layer 3 interfaces on the OLT network side	Forwarding Dynamic Host Configuration Protocol (DHCP) and broadband packets: ● VLAN ID: 2004 ● Port number: 0/4/0 ● IP address: 11.11.11.10/24 Forwarding cable modem (CM) management, VoD, COPS, and multicast packets: ● VLAN ID: 2005 ● Port number: 0/5/0 ● IP address: 11.11.12.10/24
Layer 3 interfaces connecting the router to the OLT	● Forwarding DHCP and broadband packets: 11.11.11.11 ● Forwarding CM management, VoD, COPS, and multicast packets: 11.11.12.11 ● COPS gateway IP address: 192.168.60.1

Copyright © Huawei Technologies Co., Ltd.

Item	IP Address
Upper-layer servers of the OLT	● DHCP servers: – DHCP server assigning IP addresses to CMs and media terminal adapters (MTAs): 192.168.10.10-192.168.10.11 – DHCP server assigning IP addresses to PCs and set top boxes (STBs): 192.168.10.12-192.168.10.13 ● CM management system, VoD server, and multicast server: 192.168.20.10-192.168.20.12 ● Softswitch or IP multimedia subsystem (IMS) server: 192.168.50.10

Procedure

Step 1 Create Layer 3 VLAN interfaces on the network side.

1. Create VLANs and configure their uplink ports.
   - VLAN 2004 is of the smart VLAN type and used for forwarding DHCP and broadband packets. Add uplink port 0/4/0 to VLAN 2004.
   - VLAN 2005 is of the smart VLAN type and used for forwarding CM management, VoD, and multicast packets. Add uplink port 0/5/0 to VLAN 2005.

```
huawei(config)#vlan 2004 to 2005 smart
huawei(config)#port vlan 2004 0/4 0
huawei(config)#port vlan 2005 0/5 0
```

2. (Optional) Create native VLANs for Ethernet outbound ports.

   Packets between the OLT and its upper-layer router are assumed to be forwarded at Layer 3 and no VLAN information is required. The created native VLANs remove VLAN tags from the packets transmitted out of Ethernet ports.

```
huawei(config)#interface eth 0/4
huawei(config-if-eth-0/4)#native-vlan 0 vlan 2004    //Remove VLAN tags from
the packets transmitted out of the 0/8/0 port.
huawei(config-if-eth-0/4)#quit
huawei(config)#interface eth 0/5
huawei(config-if-eth-0/5)#native-vlan 0 vlan 2005    //Remove VLAN tags from
the packets transmitted out of the 0/9/0 port.
huawei(config-if-eth-0/5)#quit
```

3. Create Layer 3 VLAN interfaces.
   a. Create a Layer 3 interface for VLAN 2004, through which DHCP and broadband packets are forwarded.

```
huawei(config)#interface vlanif 2004
huawei(config-if-vlanif2004)#ip address 11.11.11.10 255.255.255.0
huawei(config-if-vlanif2004)#quit
```

   b. Create a Layer 3 interface for VLAN 2005, through which CM management and VoD packets are forwarded.

```
huawei(config)#interface vlanif 2005
huawei(config-if-vlanif2005)#ip address 11.11.12.10 255.255.255.0
huawei(config-if-vlanif2005)#quit
```

Step 2 Configure static routes to implement the communication between the OLT and its upper-layer devices.

Copyright © Huawei Technologies Co., Ltd.

```
huawei(config)#ip route-static 0.0.0.0 0.0.0.0 11.11.11.11     //Broadband packets
are forwarded through the Layer 3 interface of VLAN 2004.
huawei(config)#ip route-static 192.168.20.0 255.255.255.0 11.11.12.11     //CM
management, VoD, and multicast packets are forwarded through the Layer 3 interface
of VLAN 2005.
huawei(config)#ip route-static 192.168.10.0 255.255.255.0 11.11.11.11     //DHCP
packets are forwarded through the Layer 3 interface of VLAN 2004.
huawei(config)#ip route-static 192.168.50.0 255.255.255.0 11.11.12.11
```

NOTE

- The interconnected router must set static routes and add the routes to dynamic routes.

----End

Result

The OLT can communicate with its upper-layer devices. To check network connectivity between two devices, run the **ping** and **tracert** commands.

The configured static routes can be queried in an IPv4 routing table by running the **display ip routing-table** command.

16.3.1.5 Configuring DHCP Relay (IPv6)

This section describes how to configure DHCPv6 relay so that terminals can obtain IP addresses in different network segments.

Prerequisites

The upper-layer router, DHCP server server of an OLT have been configured.

Data Plan

Table 16-8 DHCP data plan

Configuration Item	Data
Terminal-side of CM	● network segment of CM: 2001:0db8:0001::/64 ● network segment of PCs with fees paid: 2001:0db8:0003::/64 ● network segment of overdue PCs: 2001:0db8:0004::/64
User-side of OLT	● IP address of the gateway for the DHCP domain of CMs: 2001:0db8:0001::1/64; domain name: **docsis** ● IP address of the gateway for the DHCP domain of PCs with fees paid: 2001:0db8:0003::3/64; domain name: **default** ● IP address of the gateway for the DHCP domain of overdue PCs: 2001:0db8:0004::4/64; domain name: **default**

Copyright © Huawei Technologies Co., Ltd.

Configuration Item	Data
Network-side of OLT	Forwarding DHCP and broadband packets: ● VLAN ID: 2004 ● Port number: 0/4/0 ● IP address: 2001:0db8:0007::12/64 Forwarding CM management packets, multicast packets, and VoD packets: ● VLAN ID: 2005 ● Port number: 0/5/0 ● IP address: 2001:0db8:0008::13/64
Router	● IP address of the Layer 3 interface for forwarding DHCP and broadband packets: 2001:0db8:0007::6/64 ● IP address of the Layer 3 interface for forwarding CM management packets: 2001:0db8:0008::7/64
Server	● IP addresses of DHCP servers: – DHCP server allocating IP addresses for CMs: 2001:0db8:0006::8/64-2001:0db8:0006::9/64 – DHCP server allocating IP addresses for PCs: 2001:0db8:0006::10/64-2001:0db8:0006::11/64 ● IP addresses of the CM management system: 2001:0db8:0011::14/64-2001:0db8:0011::16/64

Procedure

Step 1 Configure the IP address of the VLAN Layer 3 interface.

```
huawei(config)#ipv6      //Enable IPv6 packet forwarding.
huawei(config)#vlan 100
huawei(config)#interface vlanif 100
huawei(config-if-vlanif100)#ipv6 enable     //Enable IPv6 on ports.
huawei(config-if-vlanif100)#undo ipv6 nd ra halt       //enables a router to send
RA messages.
huawei(config-if-vlanif100)#ipv6 nd autoconfig managed-address-flag     //Configure
the state-based auto-configuration address flag bit. The host obtains an IPv6
address using the state-based automatic configuration.
huawei(config-if-vlanif100)#ipv6 address 2001:0db8:0001::1/64     //Configure the
IP address of the gateway for the DHCP domain of CMs.
huawei(config-if-vlanif100)#ipv6 address 2001:0db8:0003::3/64     //Configure the
IP address of the gateway for the DHCP domain of PCs with fees paid.
huawei(config-if-vlanif100)#ipv6 address 2001:0db8:0004::4/64     //Configure the
IP address of the gateway for the DHCP domain of overdue PCs.
huawei(config-if-vlanif100)#quit
```

Step 2 Enable duplicate address detect (DAD) proxy, which prevents repeated link local addresses (LLAs) on the user side.

After receiving a DAD packet sent from the user side with destination IP address LLA, the OLT with DAD proxy enabled checks user online information based on the destination IP address and VLAN. If a user with the same IP address in the VLAN has been online, the OLT makes a

Copyright © Huawei Technologies Co., Ltd.

response and prohibits the new user from going online. Otherwise, the OLT does not make a response.

```
huawei(config)#ipv6 dad proxy enable
huawei(config)#vlan service-profile profile-id 10
huawei(config)#vlan bind service-profile 100 profile-id 10
huawei(config-vlan-srvprof-10)#ipv6 dad proxy enable     //DAD proxy takes effect after it is enabled at system level and VLAN service profile level.
```

Step 3 Configure the working mode of DHCP relay to Layer 3 Option 16.

Option 16 is an option with code 16 in DHCPv6 packets, which identifies terminal types. In DHCPv6 Option 16 mode, packets select a DHCPv6 server based on the Option 16 domain. Therefore, in DHCPv6 Option 16 mode, packets select a DHCPv6 server based on terminal types.

```
huawei(config)#dhcpv6 mode layer-3 option16
  Several minutes may be required and no action can be taken during this period
  Are you sure to perform this operation? (y/n)[n]: y
```

Step 4 Configure the IP addresses of the servers in a DHCP server group.

```
huawei(config)#dhcpv6-server 0 ipv6 2001:0db8:0006::8/64 2001:0db8:0006::9/64    //Configure DHCP server group 0 to allocate IP addresses for CMs.
huawei(config)#dhcpv6-server 1 ipv6 2001:0db8:0006::10/64 2001:0db8:0006::11/64    //Configure DHCP server group 1 to allocate IP addresses for PCs.
```

Step 5 Create DHCP Option 16 domains.

```
huawei(config)#dhcp domain default   //Create Option 16 domain default for PCs.
huawei(config-dhcp-domain-default)#dhcpv6-gateway learning enable   //PCs require different IP address segments based on fee payment state. Therefore, automatic gateway learning must be enabled on the OLT.
huawei(config-dhcp-domain-default)#dhcpv6-server 1 vlan 100        /Bind DHCP server group 1 to the DHCP domain of PCs. After the configuration, the PCs in this DHCP domain are mapped to DHCP server group 1.
huawei(config-dhcp-domain-default)#quit
huawei(config)#dhcp domain docsis   //Create Option 16 domain docsis for CMs.
huawei(config-dhcp-domain-docsis)#dhcpv6-server 0 vlan 100      //Bind DHCP server group 0 to the DHCP domain of CMs. After the configuration, the CMs in this DHCP domain are mapped to DHCP server group 0.
huawei(config-dhcp-domain-docsis)#quit
```

Step 6 Configure the IP addresses of the gateways for DHCP domains.

```
huawei(config)#interface vlanif 100
huawei(config-if-vlanif100)#dhcp domain default gateway ipv6 2001:0db8:0003::3/64 2001:0db8:0004::4/64    //Configure IP addresses of the gateways for the DHCP domain of PCs, including the IP address of the gateway for the PCs with fees paid and the IP address of the gateway for overdue PCs.
huawei(config-if-vlanif100)#dhcp domain docsis gateway ipv6 2001:0db8:0001::1/64    //Configure the IP address of the gateway for the DHCP domain of CMs.

huawei(config-if-vlanif100)#quit
```

----End

16.3.1.6 Configuring a Route (IPv6)

This section describes how to implement network communication by configuring a route in Layer 3 networking with an OLT. Through the route, the OLT can forward packets at Layer 3 between the OLT and its upper-layer devices or servers.

Copyright © Huawei Technologies Co., Ltd.

Prerequisites

The upper-layer router of the OLT has been configured.

Data Plan

Table 16-9 DHCP data plan

Configuration Item	Data
Terminal-side of CM	● network segment of CM: 2001:0db8:0001::/64 ● network segment of PCs with fees paid: 2001:0db8:0003::/64 ● network segment of overdue PCs: 2001:0db8:0004::/64
User-side of OLT	● IP address of the gateway for the DHCP domain of CMs: 2001:0db8:0001::1/64; domain name: **docsis** ● IP address of the gateway for the DHCP domain of PCs with fees paid: 2001:0db8:0003::3/64; domain name: **default** ● IP address of the gateway for the DHCP domain of overdue PCs: 2001:0db8:0004::4/64; domain name: **default**
Network-side of OLT	Forwarding DHCP and broadband packets: ● VLAN ID: 2004 ● Port number: 0/4/0 ● IP address: 2001:0db8:0007::12/64 Forwarding CM management packets, multicast packets, and VoD packets: ● VLAN ID: 2005 ● Port number: 0/5/0 ● IP address: 2001:0db8:0008::13/64
Router	● IP address of the Layer 3 interface for forwarding DHCP and broadband packets: 2001:0db8:0007::6/64 ● IP address of the Layer 3 interface for forwarding CM management packets: 2001:0db8:0008::7/64
Server	● IP addresses of DHCP servers: – DHCP server allocating IP addresses for CMs: 2001:0db8:0006::8/64-2001:0db8:0006::9/64 – DHCP server allocating IP addresses for PCs: 2001:0db8:0006::10/64-2001:0db8:0006::11/64 ● IP addresses of the CM management system: 2001:0db8:0011::14/64-2001:0db8:0011::16/64

Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Create VLAN Layer 3 interfaces on the network side.

1. Create VLANs and add an uplink port to them, respectively.
   - VLAN 2004 used for forwarding DHCP and broadband packets is a smart VLAN. Add uplink port 0/4/0 to VLAN 2004.
   - VLAN 2005 used for forwarding CM management packets, multicast packets, and VoD packets is a smart VLAN. Add uplink port 0/5/0 to VLAN 2005.

```
huawei(config)#vlan 2004 to 2005 smart
huawei(config)#port vlan 2004 0/4 0
huawei(config)#port vlan 2005 0/5 0
```

2. (Optional) Create native VLANs for Ethernet outbound ports.

   Packets between the OLT and its upper-layer router are forwarded at Layer 3 and no VLAN tag is required. The created native VLANs remove VLAN tags from the packets transmitted out of Ethernet ports.

```
huawei(config)#interface eth 0/4
huawei(config-if-eth-0/4)#native-vlan 0 vlan 2004    //The packets transmitted
out of port 0/4/0 are untagged.
huawei(config-if-eth-0/4)#quit
huawei(config)#interface eth 0/5
huawei(config-if-eth-0/5)#native-vlan 0 vlan 2005    //The packets transmitted
out of port 0/5/0 are untagged.
huawei(config-if-eth-0/5)#quit
```

3. Create VLAN Layer 3 interfaces.
   a. Create the Layer 3 interface of VLAN 2004, through which DHCP and broadband packets are forwarded.

```
huawei(config)#interface vlanif 2004
huawei(config-if-vlanif2004)#ipv6 address 2001:0db8:0007::12/64
huawei(config-if-vlanif2004)#quit
```

   b. Create the Layer 3 interface of VLAN 2005, through which CM management packets, multicast packets, and VoD packets are forwarded.

```
huawei(config)#interface vlanif 2005
huawei(config-if-vlanif2005)#ipv6 address 2001:0db8:0008::13/64
huawei(config-if-vlanif2005)#quit
```

Step 2 Configure static routes for the communication between the OLT and its upper-layer devices.

```
huawei(config)#ipv6 route-static ::/0 2001:0db8:0007::6/64     //Broadband packets
are forwarded through the Layer 3 interface of VLAN 2004.
huawei(config)#ipv6 route-static 2001:0db8:0011::/64 2001:0db8:0008::7/64     //CM
management packets are forwarded through the Layer 3 interface of VLAN 2005.
huawei(config)#ipv6 route-static 2001:0db8:0006::/64 2001:0db8:0007::6/64     //
DHCP packets are forwarded through the Layer 3 interface of VLAN 2004.
```

NOTE

Configure static routes on the router connected to the OLT. In addition, add the static routes to dynamic ones.

----End

Result

The OLT can communicate with its upper-layer devices. To check network connectivity between two devices, run the **ping ipv6** and **tracert ipv6** commands.

Copyright © Huawei Technologies Co., Ltd.

The configured static routes can be queried in an IPv6 routing table by running the **display ipv6 routing-table** command.

16.3.1.7 Configuring a Management Channel Between an OLT and a D-CMTS

This section describes how to configure a management channel between an optical line terminal (OLT) and a distributed cable modem termination system (D-CMTS). After the configuration, you can log in to the D-CMTS from the OLT and configure the D-CMTS.

Prerequisites

The MA5633 management policy is set to **stand-alone**. To do so, run the **sysman centralized-mgmt primary** command.

Data Plan

Item	Data	Remarks
OLT	GE port: 0/3/0	● Do not enable both the remote software commissioning using PON upstream transmission and the remote software commissioning using GE upstream transmission. ● Ensure that the database of a newly deployed D-CMTS is empty. Otherwise, the remote software commissioning using GE upstream transmission cannot be used. ● Only the network management parameters defined in SNMPv1 and SNMPv2 are supported. ● When the D-CMTS automatically obtains management parameters, it automatically generates a default route that can be restored. However, the default route may not be proper in service configuration. Therefore, you are advised to add a new route and delete the default one after the D-CMTS management channel is available. ● After the D-CMTS automatically obtains management parameters, the remote software commissioning function is automatically disabled if configurations are issued to the D-CMTS through the U2000. To modify the D-CMTS management parameters, remotely log in to the
Management VLAN and IP address of the D-CMTS	ID of the management VLAN: 8 Type of the management VLAN: smart Management IP address: 192.168.50.2/24	

Copyright © Huawei Technologies Co., Ltd.

Item	Data	Remarks
Management profile of the D-CMTS	ID: 64 Name: snmp-profile_64 SNMP version: SNMPv2c	D-CMTS through the command line interface (CLI).

Procedure

Step 1 Configure a management channel between the OLT and the D-CMTS.

1. Configure the inband management VLAN and IP address of the OLT.

```
huawei(config)#vlan 8 smart
huawei(config)#port vlan 8 0/5 0
huawei(config)#interface vlanif 8
huawei(config-if-vlanif8)#ip address 192.168.50.1 24
huawei(config-if-vlanif8)#quit
```

2. Enable Network Admission Control (NAC) on the OLT.

```
huawei(config)#nac enable master 0/3 0
```

3. (Optional) Create an SNMP management profile.

   Perform this operation if the D-CMTS is managed through the U2000. Plan an SNMP management profile on the U2000 and D-CMTS before creating the profile.

```
huawei(config)#snmp-profile add profile-id 64 profile-name snmp-profile_64 v2c
public
private 192.168.50.55 30000 trapstatus
```

4. Configure D-CMTS management parameters on the OLT.

```
huawei(config)#nac config master 0/3/0 slave vlan 8 priority 6 ip-address
192.168.50.2 mask 255.255.255.0 gateway 192.168.50.1 snmp-profile-id 64
```

   Check whether the D-CMTS management parameters have been configured on the OLT.

```
huawei(config)#display nac configuration master
{ <cr>|frameid/slotid/portid<S><Length 1-255>|frameid/slotid<S><Length
```


Copyright © Huawei Technologies Co., Ltd.

```
1-15> }:

  Command:
          display nac configuration master

------------------------------------------------------------------------------
  Frame ID/Slot ID/Port ID :  0/3/0
  VLAN                     :  8
  VLAN priority            :  3
  IP address               :  192.168.50.2
  Mask                     :  255.255.255.0
  Gateway                  :  192.168.50.254
  Snmp-profile-id          :  64
  Snmp-profile-name        :  snmp-profile_64

------------------------------------------------------------------------------
Total: 1
```

Step 2 Check whether the management channel between the OLT and the D-CMTS is available.

Upon power-on, the D-CMTS exchanges data with the OLT to obtain the management parameters.

- Run the **ping *192.168.50.2*** command on the OLT to check whether the D-CMTS can communicate with the OLT. If the OLT can receive Internet Control Message Protocol (ICMP) ECHO-REPLY packets sent from the D-CMTS, the D-CMTS is connected to the OLT.
- Run the **telnet** command on the OLT to remotely log in to the ONU from the OLT to perform the configuration. The user name is root and the password is mduadmin.

----End

16.3.1.8 Configuring a Service Channel Between an OLT and a D-CMTS

This section describes how to configure a service channel between an optical line terminal (OLT) and a distributed cable modem termination system (D-CMTS). After the configuration, the service channel forwards service packets on the D-CMTS based on the planned VLAN and forwarding policy.

Data Plan

Item	Data
High-speed Internet (HSI), VoD, broadband TV (BTV), or dynamic PacketCable service	ID of the OLT VLAN (transparently transmitting D-CMTS packet tags): 100 ID of the D-CMTS VLAN: 100 ID of the common open policy service (COPS) connection VLAN: 1000
Uplink ports	Forwarding Dynamic Host Configuration Protocol (DHCP) and broadband packets: 0/4/0 Forwarding cable modem (CM) management, VoD, and multicast packets: 0/5/0

Copyright © Huawei Technologies Co., Ltd.

Procedure

- Configure a channel for a home service.
  1. Configure service flows to receive and transparently transmit D-CMTS packets.

     The following configurations are used as an example to configure service flows:
     - Configuration of a service flow:
       - Service flow ID: 1
       - S-VLAN ID: 100
       - Customer VLAN (C-VLAN) ID: 100
     - Configuration of a COPS connection service flow:
       - Service flow ID: 2
       - VLAN (shared with the S-VLAN) ID: 100
       - C-VLAN ID: 1000
     - Device where upstream and downstream packet rates are limited: D-CMTS

       In this case, use the default traffic profile with ID 6, which does not limit the rate of a service flow. To limit packet rates, run the **traffic table ip** command to create a traffic profile and bind it to the service flow.
     - C-VLAN and S-VLAN of the D-CMTS: same

     ```
     huawei(config)#service-port 1 vlan 100 eth 0/3/0 multi-service
     user-vlan 100 rx-cttr 6 tx-cttr 6
     huawei(config)#service-port 2 vlan 100 eth 0/3/0 multi-service
     user-vlan 1000 rx-cttr 6 tx-cttr 6
     ```

     NOTE

     - On IPv6 networks, run the **dhcpv6-option permit-forwarding port 0/3/0 enable** command to enable DHCPv6 Option forwarding on a specified port.
     - If CPEs support IPv6 prefixes, run the **security bind-route-nd enable** command to enable associated routes and neighbor entries. Then, the OLT automatically generates the routing and neighbor entries of a DHCPv6 user based on the user information recorded when the user goes online. This prevents the need of manually configuring static routes and sending neighbor discovery (ND) packets to the user side, thereby improving system security.
  2. Configure the maximum number of dialup users allowed on a service port.

     For functions (such as, MAC address spoofing, anti-IP spoofing, anti-IPv6 spoofing, DHCP Proxy, IP Aware, IPoE single-MAC, VMAC DHCP aging, NS proxy response, ARP proxy response, DAD proxy, and DHCPv6 associated routes) depending on dialup operations performed by DHCP, DHCPv6, PPPoE, and SLAAC users, run this command to restrict the number of users allowed on each service port.

     ```
     huawei(config)#security user max-user-count service-port 1 2048
     huawei(config)#security user max-user-count service-port 2 2048
     ```
  3. Configure multicast cascading port 0/3/0.

     ```
     huawei(config)#btv
     huawei(config-btv)#igmp cascade-port 0/3/0
     huawei(config-btv)#quit
     ```
  4. Configure the Internet Group Management Protocol (IGMP) version to IGMPv3.

     ```
     huawei(config)#multicast-vlan 100
     huawei(config-mvlan100)#igmp version v3
     ```
  5. Configure the multicast uplink port to 0/5/0.

     ```
     huawei(config-mvlan100)#igmp uplink-port 0/5/0
     ```


Copyright © Huawei Technologies Co., Ltd.

6. Configure a multicast program generation mode.

   For the D-CMTS, the multicast programs are dynamically generated.

```
huawei(config-mvlan100)#igmp mode off
  Are you sure to close IGMP? (y/n)[n]:y
huawei(config-mvlan100)#igmp match mode disable
```

7. Configure the IGMP mode to IGMP proxy.

```
huawei(config-mvlan100)#igmp mode proxy
  Are you sure to change IGMP mode?(y/n)[n]:y
huawei(config-mvlan100)#quit
```

----End

16.3.1.9 Configuring RF Port Parameters on a D-CMTS

Radio frequency (RF) port parameters define the frequency spectrum range for signal transmission and modulation mode. The configuration of RF port parameters implements data service transmission over cables.

Data Plan

Table 16-10 Data plan for RF port parameters

Item	Data
RF port	0/1/0
Upstream channels	● IDs: 1-4 ● Type: European standard (default channel type) ● ID of the upstream channel modulation profile: 1 (by default) ● Channel central frequency (MHz): 29.8, 42.60, 49.00, and 55.4
Downstream channels	● IDs: 1-16 ● Type: European standard (default channel type) ● Channel central frequency (MHz): 602.00, 610.00, 618.00, ..., and 722.00

Procedure

- Log in to and configure the ONU.

  You can remote log in to the ONU from the OLT to perform the configuration. The user name is **root** and the password is **mduadmin**.

- Customize RF port parameters in cable mode.
  1. Configure the frequency spectrum range and channel type.

     In this example, the channel is of the European type. To change the type to North American, run the **cable** command.
  2. Configure RF port parameters for upstream channels and activate the upstream channels.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
frequency and **channel-width**	A central frequency and a frequency bandwidth determine a frequency range, within which packets are transmitted. For example, the central frequency of a European channel is 55 MHz and the frequency bandwidth is 6400 kHz. Then the frequency range of the channel is 51.8-58.2 MHz.
modulation-profile	An upstream channel modulation profile defines parameters for processing the signals transmitted over the upstream channel. You do not need to configure an upstream channel modulation profile generally. Ports automatically bind to profile 1 by default.

The following configurations are used as an example to configure RF port parameters:

- Number of upstream channels: 4
- Frequency bandwidth of the channels: 3.2 MHz (default value)

```
huawei(config)#interface cable 0/1/0
huawei(config-if-cable-0/1/0)#cable upstream 1 frequency 29.8 enable
huawei(config-if-cable-0/1/0)#cable upstream 2 frequency 42.60 enable
huawei(config-if-cable-0/1/0)#cable upstream 3 frequency 49.00 enable
huawei(config-if-cable-0/1/0)#cable upstream 4 frequency 55.40 enable
```

3. Configure RF port parameters for downstream channels and activate the downstream channels.

Parameter	Description
modulation	A greater modulation mode value for downstream channels results in a higher channel bandwidth but weaker anti-interference capability. Therefore, configure the modulation mode based on site requirements. The default modulation mode is QAM256. This example uses the default setting.

The following configuration is used as an example to configure RF parameters for downstream channels: A total of 16 downstream channels have been purchased.

```
huawei(config-if-cable-0/1/0)#cable downstream 1 frequency 602.00 enable
huawei(config-if-cable-0/1/0)#cable downstream 2 frequency 610.00 enable
huawei(config-if-cable-0/1/0)#cable downstream 3 frequency 618.00 enable
huawei(config-if-cable-0/1/0)#cable downstream 4 frequency 626.00 enable
huawei(config-if-cable-0/1/0)#cable downstream 5 frequency 634.00 enable
huawei(config-if-cable-0/1/0)#cable downstream 6 frequency 642.00 enable
huawei(config-if-cable-0/1/0)#cable downstream 7 frequency 650.00 enable
```


Copyright © Huawei Technologies Co., Ltd.

```
huawei(config-if-cable-0/1/0)#cable downstream 8 frequency 658.00 enable
huawei(config-if-cable-0/1/0)#cable downstream 9 frequency 666.00 enable
huawei(config-if-cable-0/1/0)#cable downstream 10 frequency 674.00 enable
huawei(config-if-cable-0/1/0)#cable downstream 11 frequency 682.00 enable
huawei(config-if-cable-0/1/0)#cable downstream 12 frequency 690.00 enable
huawei(config-if-cable-0/1/0)#cable downstream 13 frequency 698.00 enable
huawei(config-if-cable-0/1/0)#cable downstream 14 frequency 706.00 enable
huawei(config-if-cable-0/1/0)#cable downstream 15 frequency 714.00 enable
huawei(config-if-cable-0/1/0)#cable downstream 16 frequency 722.00 enable
```

----End

Result

1. The transmit power of the downstream channels meets site requirements.

   Run the **display cable downstream** *frameid/slotid/portid* { **all** | *channel-id* } **status** command to check whether the RF port parameters meet site requirements.

2. The signal-to-noise (SNR) ratio of the upstream channels meets site requirements.

   Run the **display cable signal quality** [*frameid/slotid/portid* [**upstream** *channel-id*]] command to check whether the RF port parameters meet site requirements. A greater SNR ratio results in better signal quality. The recommended SNR ratio is greater than 30 dB.

16.3.1.10 Configuring the HSI Service on a D-CMTS

A cable modem (CM) connects to a distributed cable modem termination system (D-CMTS) through a cable and provides the high-speed Internet (HSI) service for users.

Data Plan

Table 16-11 Data plan for the high-speed Internet (HSI) service

Item	Data
VLAN	ID of the HSI service VLAN (S-VLAN): 100; type of the VLAN: smart
Uplink port	0/0/1

Procedure

Step 1 Log in to and configure the ONU.

You can remote log in to the ONU from the OLT to perform the configuration. The user name is **root** and the password is **mduadmin**.

Step 2 Create an S-VLAN.

The S-VLAN is a user-side service VLAN between the optical line terminal (OLT) and the distributed cable modem termination system (D-CMTS). The OLT works in Layer 3 forwarding mode.

```
huawei(config)#vlan 100 smart
huawei(config)#port vlan 100 0/0 1
```


Copyright © Huawei Technologies Co., Ltd.

Step 3 Create a cable modem (CM) S-VLAN.

The CM S-VLAN identifies a CM service flow. After the CM S-VLAN is configured, the OLT automatically creates a CM service flow when the CM goes online.

```
huawei(config)#cable service-vlan 100
  Info: The new service VLAN will take effect after the CM is restarted, are you
 sure to modify? (y/n)[n]:y
```

----End

16.3.1.11 Configuring the DOCSIS VoD Service on a D-CMTS

A cable modem (CM) connects to a distributed cable modem termination system (D-CMTS) through a cable and provides the DOCSIS VoD service for users.

Context

All home services use a service VLAN (S-VLAN) and the S-VLAN is globally configured. If the S-VLAN has been configured for other home services, use the S-VLAN for the VoD service.

Data Plan

Table 16-12 Data plan for the VoD service

Item	Data
VLAN	ID of the VoD S-VLAN: 100; type of the VLAN: smart
Uplink port	0/0/1

Procedure

Step 1 Log in to and configure the ONU.

You can remote log in to the ONU from the OLT to perform the configuration. The user name is **root** and the password is **mduadmin**.

Step 2 Create an S-VLAN.

The S-VLAN is a user-side service VLAN between the optical line terminal (OLT) and the distributed cable modem termination system (D-CMTS). The OLT works in Layer 3 forwarding mode.

```
huawei(config)#vlan 100 smart
huawei(config)#port vlan 100 0/0 1
```

Step 3 Create a cable modem (CM) S-VLAN.

The CM S-VLAN identifies a CM service flow. After the CM S-VLAN is configured, the OLT automatically creates a CM service flow when the CM goes online.

Copyright © Huawei Technologies Co., Ltd.

```
huawei(config)#cable service-vlan 100
  Info: The new service VLAN will take effect after the CM is restarted, are you
 sure to modify? (y/n)[n]:y
```

----End

16.3.1.12 Configuring the EQAM VoD Service on a D-CMTS

If the MA5633 is equipped with a built-in EQAM module, the MA5633 sets idle downstream DOCSIS channels as EQAM channels to transmit VoD data.

Prerequisites

The MA5633 supports built-in EQAM.

Context

In multiservice operator (MSO)-oriented solutions, both HFC networks and STBs use the broadcast television QAM technology and support only RF signals.

Video data is encapsulated into IP and UDP packet headers that are transmitted on IP networks, which cannot be transmitted on HFC networks. To transmit the video data on HFC networks, the video data must be modulated into RF signals using the EQAM module.

Video data transmission on HFC networks uses existing CATV coaxial cables on the HFC networks, thereby reducing network deployment costs.

Data Plan

Table 16-13 Data plan for the VoD service

Item	Data
EQAM IP address	10.10.10.10
VLAN	ID of the VoD S-VLAN: 50; type of the VLAN: smart
Uplink port	Forwarding CM management, VoD, and multicast packets: 0/0/1
EQAM channel ID	13-16
Modulation mode	QAM 64
Symbol rate	6.875
UDP port number	501-514
Access port on the OLT	0/3/0
Uplink port on the OLT	0/5/0

Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Log in to and configure the ONU.

You can remote log in to the ONU from the OLT to perform the configuration. The user name is **root** and the password is **mduadmin**.

Step 2 Configure RF port parameters.

```
huawei(config)#interface cable 0/1/0
huawei(config-if-cable-0/1/0)#cable downstream 13 frequency 698.0 modulation qam64
enable channel-mode eqam symbol-rate 6.875
huawei(config-if-cable-0/1/0)#cable downstream 14 frequency 706.00 modulation
qam64 enable channel-mode eqam symbol-rate 6.875
huawei(config-if-cable-0/1/0)#cable downstream 15 frequency 714.00 modulation
qam64 enable channel-mode eqam symbol-rate 6.875
huawei(config-if-cable-0/1/0)#cable downstream 16 frequency 722.00 modulation
qam64 enable channel-mode eqam symbol-rate 6.875
huawei(config-if-cable-0/1/0)#quit
```

Step 3 Configure a video profile.

A video profile contains all video mappings on an EQAM module and supports batch video mapping configurations. This facilitates video mapping configuration and management.

```
huawei(config)#cable eqam video profile name vod1
huawei(config-eqam-video-profile-vod1)#mapping index 1 type spts udp-port 501
output-program 1 pmtpid 32 channel 13
huawei(config-eqam-video-profile-vod1)#mapping index 2 type spts udp-port 502
output-program 2 pmtpid 48 channel 13
huawei(config-eqam-video-profile-vod1)#mapping index 3 type spts udp-port 503
output-program 3 pmtpid 64 channel 13
huawei(config-eqam-video-profile-vod1)#mapping index 4 type spts udp-port 504
output-program 4 pmtpid 80 channel 13
huawei(config-eqam-video-profile-vod1)#mapping index 5 type spts udp-port 505
output-program 1 pmtpid 96 channel 14
huawei(config-eqam-video-profile-vod1)#mapping index 6 type spts udp-port 506
output-program 2 pmtpid 112 channel 14
huawei(config-eqam-video-profile-vod1)#mapping index 7 type spts udp-port 507
output-program 3 pmtpid 128 channel 14
huawei(config-eqam-video-profile-vod1)#mapping index 8 type spts udp-port 508
output-program 1 pmtpid 160 channel 15
huawei(config-eqam-video-profile-vod1)#mapping index 9 type spts udp-port 509
output-program 2 pmtpid 176 channel 15
huawei(config-eqam-video-profile-vod1)#mapping index 10 type spts udp-port 510
output-program 1 pmtpid 224 channel 16
huawei(config-eqam-video-profile-vod1)#mapping index 11 type spts udp-port 511
output-program 2 pmtpid 240 channel 16
huawei(config-eqam-video-profile-vod1)#mapping index 12 type spts udp-port 512
output-program 3 pmtpid 256 channel 16
huawei(config-eqam-video-profile-vod1)#mapping index 13 type spts udp-port 513
output-program 4 pmtpid 272 channel 16
huawei(config-eqam-video-profile-vod1)#mapping index 14 type spts udp-port 514
output-program 5 pmtpid 288 channel 16
huawei(config-eqam-video-profile-vod1)#quit
```


Copyright © Huawei Technologies Co., Ltd.

NOTE

To configure video mappings in batches, do as follows:

```
huawei(config)#cable eqam video profile name vod1
huawei(config-eqam-video-profile-vod1)#mapping index 1 type spTS udp-port 501
output-program 1 pmtpid 32 chan
nel 13 number 4 increment output-program 1 pmtpid 32 udp-port 1
huawei(config-eqam-video-profile-vod1)#mapping index 5 type spts udp-port 505
output-program 1 pmtpid 96 chan
nel 14 number 3 increment output-program 1 pmtpid 32 udp-port 1
huawei(config-eqam-video-profile-vod1)#mapping index 8 type spts udp-port 508
output-program 1 pmtpid 160 chan
nel 15 number 2 increment output-program 1 pmtpid 32 udp-port 1
huawei(config-eqam-video-profile-vod1)#mapping index 10 type spts udp-port 510
output-program 1 pmtpid 224 chan
nel 16 number 5 increment output-program 1 pmtpid 32 udp-port 1
```

Step 4 Configure the VoD S-VLAN.

VLAN 50 is the S-VLAN that functions between the OLT and the MA5633. The OLT works in Layer 3 forwarding mode.

```
huawei(config)#vlan 50 smart
huawei(config)#port vlan 50 0/0 1
```

Step 5 Configure a video domain.

A video domain defines the relationships between an EQAM module and an EQAM IP address, and between the S-VLAN used for video data forwarding on an EQAM module, the EQAM module, and a video profile. This facilitates data management.

```
huawei(config)#cable eqam video domain huawei
huawei(config-eqam-domain-huawei)#local ip 10.10.10.10 vlan 50
huawei(config-eqam-domain-huawei)#bind video profile name vod1 0/1/0
huawei(config-eqam-domain-huawei)#quit
```

----End

Result

The MA5633 supports packet statistics query. Based on the statistical results, you can determine whether users can order programs and whether packet loss occurs in program transmitting.

- Run the **display cable eqam video stream** command to check the TS status. If the status is **online**, the TS is functional.
- Run the **display cable eqam video statistics input** command to query packet statistics and network jitter of a TS on the video service input end.

  Check whether the program ordered by a user has been sent to the MA5633. If the program has been sent to the MA5633, check whether the program traffic is normal.
- Run the **display cable eqam video statistics output** command to query packet statistics of a TS on the video service output end.

  Check whether the TS contains the ordered program, whether the program has been sent to the STB, and whether the TS traffic is normal.

Follow-up Procedure

After configuring the MA5633, perform the following steps to configure a service channel on the OLT.

Copyright © Huawei Technologies Co., Ltd.

1. Configure an S-VLAN.

   VLAN 50 is the S-VLAN that functions between the OLT and the MA5633. The OLT works in Layer 3 forwarding mode.

   ```
   OLT(config)#vlan 50 smart
   OLT(config)#port vlan 50 0/5 0
   ```

2. Configure a service flow.

   - Configuration of a service flow:
     - Service flow ID: 3
     - S-VLAN ID: 50
     - Customer VLAN (C-VLAN) ID: 50
   - Device where upstream and downstream packet rates are limited: MA5633 (In this case, use the default traffic profile with ID 6, which does not limit the rate of a service flow. To limit packet rates, run the **traffic table ip** command to create a traffic profile and bind it to the service flow.)

   Configuration if the service is accessed using a GPON board:

   ```
   OLT(config)#service-port 3 vlan 50 gpon 0/3/0 ont 1 gemport 1 multi-service
   user-vlan 50 rx-cttr 6 tx-cttr 6
   ```

   Configuration if the service is accessed using a GE board:

   ```
   OLT(config)#service-port 3 vlan 50 eth 0/3/0 multi-service
   user-vlan 50 rx-cttr 6 tx-cttr 6
   ```

16.3.1.13 Configuring the BTV Service

A cable modem (CM) connects to a distributed cable modem termination system (D-CMTS) through a cable and provides the multicast service for users.

Context

All home services use a service VLAN (S-VLAN) and the S-VLAN is globally configured. If the S-VLAN has been configured for other home services, use the S-VLAN for the multicast service.

Data Plan

Table 16-14 Data plan for the multicast service

Item	Data
VLAN	ID of the multicast S-VLAN: 100; type of the VLAN: smart
Uplink ports	0/0/1

Procedure

Step 1 Log in to and configure the ONU.

Copyright © Huawei Technologies Co., Ltd.

You can remote log in to the ONU from the OLT to perform the configuration. The user name is **root** and the password is **mduadmin**.

Step 2 Create an S-VLAN.

The S-VLAN is a user-side service VLAN between the optical line terminal (OLT) and the distributed cable modem termination system (D-CMTS). The OLT works in Layer 3 forwarding mode.

```
huawei(config)#vlan 100 smart
huawei(config)#port vlan 100 0/0 1
```

Step 3 Create a cable modem (CM) S-VLAN.

The CM S-VLAN identifies a CM service flow. After the CM S-VLAN is configured, the OLT automatically creates a CM service flow when the CM goes online.

```
huawei(config)#cable service-vlan 100
  Info: The new service VLAN will take effect after the CM is restarted, are you
 sure to modify? (y/n)[n]:y
```

Step 4 Configure multicast VLAN 100.

NOTE

This configuration takes effect only after the CMs go online again.

```
huawei(config)#multicast-vlan 100
```

Step 5 Configure the Internet Group Management Protocol (IGMP) version to IGMPv3.

```
huawei(config-mvlan100)#igmp version v3
```

Step 6 Configure a multicast program generation mode.

Multicast programs can be dynamically or statically generated. For the D-CMTS, the multicast programs are dynamically generated.

```
huawei(config-mvlan100)#igmp mode off
  Are you sure to close IGMP? (y/n)[n]:y
huawei(config-mvlan100)#igmp match mode disable
```

Step 7 Configure the multicast uplink port to 0/0/1.

```
huawei(config-mvlan100)#igmp uplink-port 0/0/1
```

Step 8 Configure the IGMP mode to IGMP proxy.

```
huawei(config-mvlan100)#igmp mode proxy
  Are you sure to change IGMP mode?(y/n)[n]:y
huawei(config-mvlan100)#quit
```

Step 9 Bind CM multicast users to the multicast VLAN.

NOTE

This configuration takes effect only after the CMs go online again.

```
huawei(config)#cable multicast-vlan 100
```

Step 10 (Optional) Disable multicast DSID-based forwarding (MDF).

Multicast DSID-based forwarding is defined in data over cable service interface specification (DOCSIS) 3.0, perform this step if the CMs comply with DOCSIS 2.0.

Disable MDF if the CMTS is connected to a CM equipped with a TI chip. Otherse, the CM may go online and offline repeatedly.

Copyright © Huawei Technologies Co., Ltd.

```
huawei(config)#cable multicast mdf disable
```

Step 11 (Optional) Configure multicast user authentication.

NOTE

Perform this step if the configuration file on the CM server contains only the multicast rights profile name and the multicast rights must be configured on the D-CMTS.

The following configurations are used as an example to configure multicast user authentication:

- Multicast authentication function: enabled globally
- Maximum number of programs can be ordered if the CM does not match any rights rule: 32
- IP addresses of the multicast programs that can be ordered by multicast users: 225.1.1.1 and 225.1.1.2
- IP address of the multicast server: 192.168.20.11
- Multicast program priorities: 254 and 255

```
huawei(config)#cable multicast authorization enable max-sessions 32 default-acti
on permit
huawei(config)#cable multicast auth-profile profile-name btv1
huawei(config-multicast-profile-btv1)#rule 1 priority 255 group-ip 225.1.1.1 gro
up-ip-mask 24 src-ip 192.168.20.11 src-ip-mask 24 permit
huawei(config-multicast-profile-btv1)#rule 1 priority 254 group-ip 225.1.1.2 gro
up-ip-mask 24 src-ip 192.168.20.11 src-ip-mask 24 permit
```

Step 12 (Optional) Configure cable multicast version.

```
huawei(config)#cable multicast igmp-version v3
```

----End

16.3.1.14 Configuring the Dynamic PacketCable Service on a D-CMTS

A cable modem (CM) connects to a distributed cable modem termination system (D-CMTS) through a cable and provides the dynamic PacketCable service for users.

Context

Table 16-15 Data plan for the PacketCable service

Item	Data
Uplink port	0/0/1
VLAN	ID of the PacketCable service VLAN (S-VLAN): 100; type of the VLAN: smart ID of the common open policy service (COPS) connection VLAN: 1000
IP address for creating a COPS connection to an IP multimedia subsystem (IMS) or a softswitch	192.168.60.3/24 (in the same network segment as the IMS or softswitch or can communicate with the IMS or softswitch)

Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Log in to and configure the ONU.

You can remote log in to the ONU from the OLT to perform the configuration. The user name is **root** and the password is **mduadmin**.

Step 2 Create a service VLAN (S-VLAN).

NOTE

All home services use an S-VLAN and the S-VLAN is globally configured. If the S-VLAN has been configured for other home services, use the S-VLAN in steps **Step 1** and **Step 2**.

The S-VLAN is a user-side service VLAN between the optical line terminal (OLT) and the D-CMTS. The OLT works in Layer 3 forwarding mode.

```
huawei(config)#vlan 100 smart
huawei(config)#port vlan 100 0/0 1
```

Step 3 Create a cable modem (CM) S-VLAN.

The CM S-VLAN identifies a CM service flow. After the CM S-VLAN is configured, the OLT automatically creates a CM service flow when the CM goes online.

```
huawei(config)#cable service-vlan 100
  Info: The new service VLAN will take effect after the CM is restarted, are you
 sure to modify? (y/n)[n]:y
```

Step 4 Configure the Layer 3 interface for COPS connections.

```
huawei(config)#vlan 1000 smart
huawei(config)#interface vlanif 1000
huawei(config-if-vlanif1000)#ip address 192.168.60.3 24
huawei(config-if-vlanif1000)#quit
huawei(config)#port vlan 1000 0/0 1
```

Step 5 Configure a COPS connection.

The following configurations are used as an example to configure a COPS connection:

- COPS policy enforcement point (PEP) ID: IP address of the Layer 3 interface for the COPS connection
- Transmit and receive buffer for TCP sockets: 12 KB
- Differentiated services code point (DSCP) priority of COPS packets: ef

```
huawei(config)#cops pepid 192.168.60.3
huawei(config)#cops tcp window 12
huawei(config)#cops ip dscp ef
```

Step 6 Configure PacketCable parameters.

PacketCable 1.x parameter settings are as follows:

- Embedded media terminal adapter (EMTA) creating a dynamic media stream: permitted
- Other parameters: default settings

```
huawei(config)#packetcable 1dotx enable
huawei(config)#packetcable authorize common-docsis-mta enable
huawei(config)#packetcable multimedia enable
```

----End

Copyright © Huawei Technologies Co., Ltd.

16.3.1.15 Verifying Services

To facilitate service verification, an MA5633 supports multiple remote service verification methods, such as Dynamic Host Configuration Protocol (DHCP) dialup emulation tests. This allows commissioning and configuration engineers to remotely verify services. In addition, this section describes how to verify services on site.

Prerequisites

- The MA5633 is properly connected to the upper-layer network.
- The DHCP server, Trivial File Transfer Protocol (TFTP) server, and softswitch or IP multimedia subsystem (IMS) have been configured.

Procedure

- Log in to and configure the ONU.

  You can remote log in to the ONU from the OLT to perform the configuration. The user name is **root** and the password is **mduadmin**.

- Perform a DHCP dialup emulation test.

  In this test, a cable modem (CM) is emulated on the MA5633 to apply to the DHCP server for an IP address. This checks whether the MA5633 can communicate with the DHCP server and verifies CM DHCP configurations on the DHCP relay, proxy, and server.

  1. Run the **simulate dhcp start cm** *mac-address* [**option60** *option60*] command to start a DHCP dialup emulation test.

     NOTE

     You can run the **simulate dhcp stop** command to stop the DHCP emulation.

  2. Run the **display simulation dhcp** command to query the results of the DHCP dialup emulation test.
  3. Check whether the **User IP** has obtained an IP address.

- Check the CM status.

  Run the **display cable modem** command to query the CM status in **Status**.

```
huawei(config)#display cable modem  all

------------------------------------------------------------------------------
-
 Idx   MAC            IP              I/F          Status   Prim  Num Ver  DS
RX
                                                           SID   CPE
Power

------------------------------------------------------------------------------
-
 1     0023-ED6F-21A3 192.168.1.118   0/1/0/U4     ol-pt    1     0   D2.0
-

------------------------------------------------------------------------------
-
 Total:
1
 ol: 0, ol-ptd: 0, ol-pt: 1, ol-d: 0, wol: 0, wol-ptd: 0, wol-pt: 0, wol-d:
0,
pol: 0, pol-ptd: 0, pol-pt: 0, pol-d: 0, offline: 0, rej-m: 0, rej-pt: 0, rej-
```


Copyright © Huawei Technologies Co., Ltd.

```
o:
 0, init: 0, init-rc: 0, DHCP: 0, DHCP-O: 0, DHCP-R: 0, DHCP-C: 0, REG:
0
 Note: 1. Idx is the index of a
CM.
       2. The downstream received power is in the unit of
dBmV.
       3. In status, "ol" means online, "rej" means reject.
```

The following table lists the CM status and handling suggestions.

CM Status	Description	Handling Suggestion
init	Indicates that the CM initialization ranging message is received.the CM initialization.	If a CM is always in the ranging state, the ranging fails. Then check radio frequency (RF) line indicators and detect line faults.
init-rc	Indicates that the CM initialization ranging is complete.	No action is required. The ranging of the CM is complete.
DHCP	Indicates that the DHCP discovery from the CM is received.	If a CM initiates a DHCP request but does not obtain an IP address, check the DHCP server, routing between the OLT and the DHCP server, and DHCP server parameter settings.
● DHCP-O ● DHCP-R ● DHCP-C	● DHCP-O: indicates that the offer from the DHCP server is received. ● DHCP-R: indicates that the DHCP request from the CM is received. ● DHCP-C: indicates that the acknowledge from the DHCP server is received.	The DHCP server has assigned an IP address to the CM and sent configuration file name and IP address of the TFTP or ToD server to the CM using the Option 67 and Option 66 fields (the Option 67 field carries the configuration file name and the Option 66 field carries the IP address of the TFTP or ToD server). If the CM is always in the DHCP-C state, the CM fails to obtain the configuration file. Then check the TFTP server, routing between the OLT and the TFTP server, and TFTP server parameter settings.
REG	Indicates that a registration is started.	If the CM is always in the register state, the CM obtains an incorrect configuration file. Then change the configuration file.

Copyright © Huawei Technologies Co., Ltd.

CM Status	Description	Handling Suggestion
● ol ● ol-pt ● ol-ptd ● ol-d ● wol ● wol-pt ● wol-ptd ● wol-d ● pol ● pol-pt ● pol-ptd	● ol: indicates that the CM is online. (valid only for CMs complying with DOCSIS 2.0) ● ol-pt: indicates that the CM is online and passes the BPI authentication. (valid only for CMs complying with DOCSIS 2.0) ● ol-ptd: indicates that the CM is online and passes the BPI authentication, and NetAccessEnable is disabled. (valid only for CMs complying with DOCSIS 2.0) ● ol-d: indicates that the CM is online and NetAccessEnable is disabled. (valid only for CMs complying with DOCSIS 2.0) ● wol: indicates that the CM is online and all channels bound to the CM are available. (valid only for CMs complying with DOCSIS 3.0) ● wol-pt: indicates that the CM is online and passes the BPI authentication, and all channels bound to the CM are available. (valid only for CMs complying with DOCSIS 3.0) ● wol-ptd: indicates that the CM is online and passes the BPI authentication, NetAccessEnable is disabled, and all channels bound to the CM are available. (valid only for CMs complying with DOCSIS 3.0) ● wol-d: indicates that the CM is online, NetAccessEnable is disabled, and all channels bound to the CM are available. (valid only for CMs complying with DOCSIS 3.0) ● pol: indicates that the CM is online and some channels	No action is required. The status indicates that the CM has registered

Copyright © Huawei Technologies Co., Ltd.

CM Status	Description	Handling Suggestion
● pol-d	bound to the CM are available. (valid only for CMs complying with DOCSIS 3.0) ● pol-pt: indicates that the CM is online and passes the BPI authentication, and some channels bound to the CM are available. (valid only for CMs complying with DOCSIS 3.0) ● pol-ptd: indicates that the CM is online and passes the BPI authentication, NetAccessEnable is disabled, and some channels bound to the CM are available. (valid only for CMs complying with DOCSIS 3.0) ● pol-d: indicates that the CM is online, NetAccessEnable is disabled, and some channels bound to the CM are available. (valid only for CMs complying with DOCSIS 3.0)	with the OLT and can correctly transmit and receive services.
offline	Indicates the offline status.	If the CM is in the offline state, check the power status, noise, and channel frequency of the CM.
● rej-m ● rej-pt ● rej-o	● rej-m: indicates that the MIC verification fails. ● rej-pt: indicates that the BPI authentication fails. ● rej-o: indicates that the authentication reject due to other reasons.	If the CM is in the reject state, no service flow can be created. Then check the CM authentication and CM message integrity check (MIC), and check whether class of service (COS) parameters specified in the CM configuration file are supported by the OLT.

- Verify that home services can be provisioned.
  1. After the CM is installed at a user home and commissioned, the user can watch TV programs.
  2. After the high-speed Internet (HSI) service is provisioned, the user can access the Internet from a PC.
  3. After the VoD service is provisioned, the user can order programs.
  4. After the VoIP service is provisioned, the user can make and receive phone calls.

Copyright © Huawei Technologies Co., Ltd.

5. After the multicast service is provisioned, the user can watch ordered multicast programs.

----End

16.3.2 L2VPN Enterprise Service Networking

In L2VPN enterprise service networking, an MA5633 connects to cable modems (CMs) through radio frequency (RF) ports, and the CMs connect to switches to provide the L2VPN service for users. This section describes how to configure the optical line terminal (OLT) and the MA5633 to provision the L2VPN service.

NOTE

Configuration procedures are the same for IPv6 and IPv4 networks except in "onfigure Dynamic Host Configuration Protocol (DHCP) rela" and "onfigure a route".

16.3.2.1 Service Requirements and Usage Scenario

Service Requirements

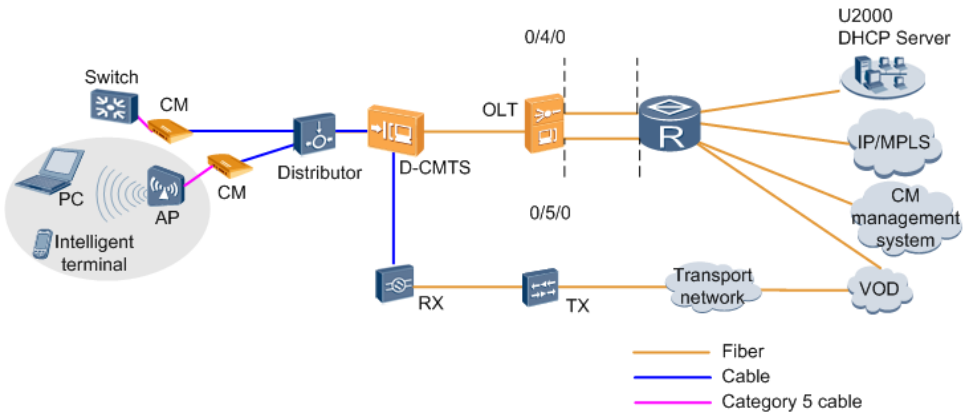
An enterprise requires the provisioning of the L2VPN service.

Usage Scenario

As shown in **Figure 16-6**, MA5633 is deployed on an optical node and cable modems (CMs) are deployed at enterprises. The CMs connect to radio frequency (RF) ports on the MA5633 through cables.

- A CM provides the enterprise service through a switch, which connects to enterprise users.
- Enterprise users access the Internet through Dynamic Host Configuration Protocol (DHCP) dialup.

Figure 16-6 L2VPN enterprise service networking

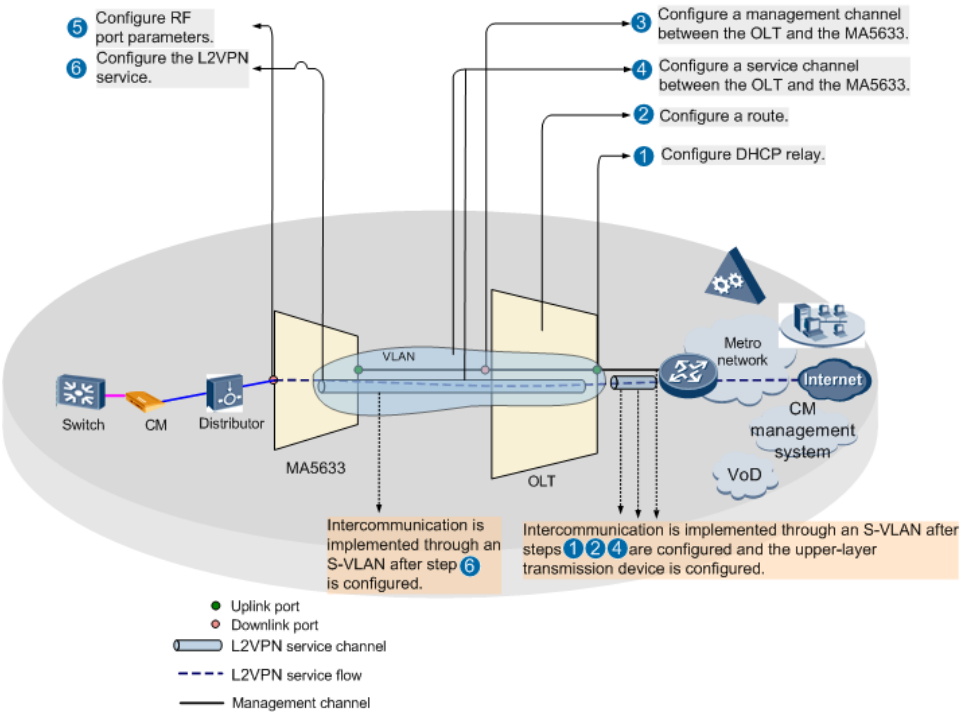


16.3.2.2 Configuration Process

Copyright © Huawei Technologies Co., Ltd.

Figure 16-7 shows the configuration roadmap for the L2VPN service networking.

Figure 16-7 Configuration roadmap for the L2VPN service networking



NOTE

Before logging in to the MA5633 to configure services on it, ensure that the MA5633 has been properly connected.

The following table describes the configuration steps.

Configuration Object	Step
Optical line terminal (OLT)	● IPv4: **Configure Dynamic Host Configuration Protocol (DHCP) relay.** ● IPv6: Configure Dynamic Host Configuration Protocol (DHCP) relay (IPv6).
	● IPv4: **Configure a route.** ● IPv6: **Configure a route (IPv6).**
	Configure a management channel between the OLT and the D-CMTS.
	Configure a service channel between the OLT and the D-CMTS.
MA5633	**Configure radio frequency (RF) port parameters.**
	Configure the L2VPN service.
	Verify the configured service.

Copyright © Huawei Technologies Co., Ltd.

16.3.2.3 Configuring DHCP Relay

This section describes how to configure Dynamic Host Configuration Protocol (DHCP) relay so that cable modems (CMs) can obtain IP addresses in different network segments.

Prerequisites

The upper-layer router, DHCP server, and Trivial File Transfer Protocol (TFTP) server of an optical line terminal (OLT) have been configured.

Data Plan

Table 16-16 DHCP data plan for the OLT

Item	Data
VLAN	ID of the CM management S-VLAN: 200; type of the VLAN: smart
DHCP server group parameters	IP address of the DHCP domain gateway for CMs: 10.10.224.1; domain name: docsis

Table 16-17 Data plan for the upper-layer devices of the OLT

Item	IP Address
Layer 3 interfaces connecting the router to the OLT	● Forwarding DHCP and broadband packets: 11.11.11.11 ● Forwarding CM management packets: 11.11.12.11
IP address of the DHCP server	DHCP server assigning IP addresses to CMs and media terminal adapters (MTAs): 192.168.10.10-192.168.10.11

Procedure

Step 1 Set the IP address of the VLAN Layer 3 interface.

```
huawei(config)#vlan 100 smart
huawei(config)#interface vlanif 100
huawei(config-if-vlanif100)#ip address 10.10.224.1 255.255.255.0     //Set the IP address of the DHCP domain gateway for CMs.
huawei(config-if-vlanif100)#quit
```

Step 2 Configure the working mode of the DHCP relay to Layer 3 Option 60.

In DHCP Option 60 mode, a DHCP server group is selected according to the Option 60 domain name in DHCP packets. Users in this mode are identified by domain information of packets, which differentiates various service types in a VLAN. Ensure that the Option 60 domain name and the DHCP server group bound to the Option 60 domain name are configured beforehand.

Copyright © Huawei Technologies Co., Ltd.

```
huawei(config)#dhcp mode layer-3 Option60
  Several minutes may be required and no action can be taken during this period
  Are you sure to perform this operation? (y/n)[n]: y
```

Step 3 Set the IP addresses of the servers in a DHCP server group.

```
huawei(config)#dhcp-server 0 ip 192.168.10.10 192.168.10.11    //Configure DHCP
server group 0 to assign IP addresses to CMs.
```

Step 4 Create a DHCP Option 60 domain.

```
huawei(config)#dhcp domain docsis   //Create Option 60 domain name docsis for CMs.
huawei(config-dhcp-domain-docsis)#dhcp-server 0 vlan 100       //Bind DHCP server
group 0 to the DHCP domain where the CMs locate. After the configuration, the CMs
in the DHCP domain are corresponded to DHCP server group 0.
huawei(config-dhcp-domain-docsis)#quit
```

Step 5 Set the IP address of the gateway for the DHCP domain.

```
huawei(config)#interface vlanif 100
huawei(config-if-vlanif100)#dhcp domain docsis gateway 10.10.224.1    //Set the IP
address of the gateway for the CM domain to 10.10.224.1.
huawei(config-if-vlanif100)#quit
```

----End

16.3.2.4 Configuring a Route

This section describes how to implement network communication by configuring a route in Layer 3 networking with an optical line terminal (OLT). Through the route, packets are forwarded at Layer 3 between the OLT and its upper-layer devices or servers.

Prerequisites

The upper-layer router of an OLT has been configured.

Data Plan

Table 16-18 Data plan for the Layer 3 interfaces on the network side

Item	IP Address
Layer 3 interfaces on the OLT network side	Forwarding Dynamic Host Configuration Protocol (DHCP) packets: ● VLAN ID: 2004 ● Port number: 0/4/0 ● IP address: 11.11.11.10/24 Forwarding cable modem (CM) management packets: ● VLAN ID: 2005 ● Port number: 0/5/0 ● IP address: 11.11.12.10/24
Layer 3 interfaces connecting the router to the OLT	● Forwarding DHCP packets: 11.11.11.11 ● Forwarding CM management packets: 11.11.12.11

Copyright © Huawei Technologies Co., Ltd.

Item	IP Address
Upper-layer servers of the OLT	● DHCP server assigning IP addresses to CMs and media terminal adapters (MTAs): 192.168.10.10-192.168.10.11 ● CM management system: 192.168.20.1

Procedure

Step 1 Create Layer 3 VLAN interfaces on the network side.

1. Create VLANs and configure their uplink ports.
   - VLAN 2004 is of the smart VLAN type and used for forwarding DHCP packets. Add uplink port 0/4/0 to VLAN 2004.
   - VLAN 2005 is of the smart VLAN type and used for forwarding CM management packets. Add uplink port 0/5/0 to VLAN 2005.

```
huawei(config)#vlan 2004 to 2006 smart
huawei(config)#port vlan 2004 0/4 0
huawei(config)#port vlan 2005 0/5 0
```

2. (Optional) Create native VLANs for Ethernet outbound ports.

   Packets between the OLT and its upper-layer router are forwarded at Layer 3 and no VLAN information is required. The created native VLANs remove VLAN tags from the packets transmitted out of Ethernet ports.

```
huawei(config)#interface eth 0/4
huawei(config-if-eth-0/4)#native-vlan 0 vlan 2004    //Remove VLAN tags from
the packets transmitted out of the 0/4/0 port.
huawei(config-if-eth-0/4)#quit
huawei(config)#interface eth 0/5
huawei(config-if-eth-0/5)#native-vlan 0 vlan 2005    //Remove VLAN tags from
the packets transmitted out of the 0/5/0 port.
huawei(config-if-eth-0/5)#quit
```

3. Create Layer 3 VLAN interfaces.
   a. Create a Layer 3 interface for VLAN 2004, through which DHCP packets are forwarded.

```
huawei(config)#interface vlanif 2004
huawei(config-if-vlanif2004)#ip address 11.11.11.10 255.255.255.0
huawei(config-if-vlanif2004)#quit
```

   b. Create a Layer 3 interface for VLAN 2005, through which CM management packets are forwarded.

```
huawei(config)#interface vlanif 2005
huawei(config-if-vlanif2005)#ip address 11.11.12.10 255.255.255.0
huawei(config-if-vlanif2005)#quit
```

Step 2 Configure static routes to implement the communication between the OLT and its upper-layer devices.

```
huawei(config)#ip route-static 192.168.20.0 255.255.255.0 11.11.12.11     //CM
management and VoD packets are forwarded through the Layer 3 interface of VLAN
2005.
huawei(config)#ip route-static 192.168.10.0 255.255.255.0 11.11.11.11     //DHCP
packets are forwarded through the Layer 3 interface of VLAN 2004.
```


Copyright © Huawei Technologies Co., Ltd.

NOTE

The interconnected router must set static routes and add the routes to dynamic routes.

----End

Result

The OLT can communicate with its upper-layer devices. To check network connectivity between two devices, run the **ping** and **tracert** commands.

The configured static routes can be queried in an IPv4 routing table by running the **display ip routing-table** command.

16.3.2.5 Configuring DHCP Relay (IPv6)

This section describes how to configure DHCPv6 relay so that CMs can obtain IP addresses in different network segments.

Prerequisites

The upper-layer router, DHCP server, and Trivial File Transfer Protocol (TFTP) server of an OLT have been configured.

Data Plan

Table 16-19 data plan

Configuration Item	Data
Terminal-side of CM	network segment of CM: 2001:0db8:0001::/64
User-side of OLT	IP address of the gateway for the DHCP domain of CMs: 2001:0db8:0001::1/64; domain name: **docsis**
Network-side of OLT	Forwarding DHCP and broadband packets: ● VLAN ID: 2004 ● Port number: 0/4/0 ● IP address: 2001:0db8:0007::12/64 Forwarding CM management packets, multicast packets, and VoD packets: ● VLAN ID: 2005 ● Port number: 0/5/0 ● IP address: 2001:0db8:0008::13/64
Router	● IP address of the Layer 3 interface for forwarding DHCP and broadband packets: 2001:0db8:0007::6/64 ● IP address of the Layer 3 interface for forwarding CM management packets: 2001:0db8:0008::7/64

Copyright © Huawei Technologies Co., Ltd.

Configuration Item	Data
Server	● IP addresses of DHCP servers: – DHCP server allocating IP addresses for CMs: 2001:0db8:0006::8/64-2001:0db8:0006::9/64 – DHCP server allocating IP addresses for PCs: 2001:0db8:0006::10/64-2001:0db8:0006::11/64 ● IP addresses of the CM management system: 2001:0db8:0011::14/64-2001:0db8:0011::16/64

Procedure

Step 1 Configure a CM service provisioning mode, which can be IPv6 (preferentially used), APM, or DPM (used for dual-stack service provisioning). Select a mode based on site requirements.

```
huawei(config)#interface cable 1/1/0
huawei(config-if-cable-1/1/0)#cable ip-mode dpm
huawei(config-if-cable-1/1/0)#quit
```

Step 2 Configure the IP address of the VLAN Layer 3 interface.

```
huawei(config)#ipv6      //Enable IPv6 packet forwarding.
huawei(config)#vlan 100
huawei(config)#interface vlanif 100
huawei(config-if-vlanif100)#ipv6 enable     //Enable IPv6 on ports.
huawei(config-if-vlanif100)#undo ipv6 nd ra halt       //enables a router to send
RA messages.
huawei(config-if-vlanif100)#ipv6 nd autoconfig managed-address-flag     //Configure
the state-based auto-configuration address flag bit. The host obtains an IPv6
address using the state-based automatic configuration.
huawei(config-if-vlanif100)#ipv6 address 2001:0db8:0001::1/64     //Configure the
IP address of the gateway for the DHCP domain of CMs.
huawei(config-if-vlanif100)#quit
```

Step 3 Enable duplicate address detect (DAD) proxy, which prevents repeated link local addresses (LLAs) on the user side.

After receiving a DAD packet sent from the user side with destination IP address LLA, the OLT with DAD proxy enabled checks user online information based on the destination IP address and VLAN. If a user with the same IP address in the VLAN has been online, the OLT makes a response and prohibits the new user from going online. Otherwise, the OLT does not make a response.

```
huawei(config)#ipv6 dad proxy enable
huawei(config)#vlan service-profile profile-id 10
huawei(config)#vlan bind service-profile 100 profile-id 10
huawei(config-vlan-srvprof-10)#ipv6 dad proxy enable     //DAD proxy takes effect
after it is enabled at system level and VLAN service profile level.
```

Step 4 Configure the working mode of DHCP relay to Layer 3 Option 16.

Option 16 is an option with code 16 in DHCPv6 packets, which identifies terminal types. In DHCPv6 Option 16 mode, packets select a DHCPv6 server based on the Option 16 domain. Therefore, in DHCPv6 Option 16 mode, packets select a DHCPv6 server based on terminal types.

```
huawei(config)#dhcpv6 mode layer-3 option16
  Several minutes may be required and no action can be taken during this period
  Are you sure to perform this operation? (y/n)[n]: y
```


Copyright © Huawei Technologies Co., Ltd.

Step 5 Configure the IP addresses of the servers in a DHCP server group.

```
huawei(config)#dhcpv6-server 0 ipv6 2001:0db8:0006::8/64 2001:0db8:0006::9/64    //
Configure DHCP server group 0 to allocate IP addresses for CMs.
```

Step 6 Create DHCP Option 16 domains.

```
huawei(config)#dhcp domain docsis   //Create Option 16 domain docsis for CMs.
huawei(config-dhcp-domain-docsis)#dhcpv6-server 0 vlan 100      //Bind DHCP server
group 0 to the DHCP domain of CMs. After the configuration, the CMs in this DHCP
domain are mapped to DHCP server group 0.
huawei(config-dhcp-domain-docsis)#quit
```

Step 7 Configure the IP addresses of the gateways for DHCP domains.

```
huawei(config)#interface vlanif 100
huawei(config-if-vlanif100)#dhcpv6 domain docsis gateway 2001:0db8:0001::1/64    //
Configure the IP address of the gateway for the DHCP domain of CMs.
huawei(config-if-vlanif100)#quit
```

----End

16.3.2.6 Configuring a Route (IPv6)

This section describes how to implement network communication by configuring a route in Layer 3 networking with an OLT. Through the route, the OLT can forward packets at Layer 3 between the OLT and its upper-layer devices or servers.

Prerequisites

The upper-layer router of the OLT has been configured.

Data Plan

Table 16-20 data plan

Configuration Item	Data
Terminal-side of CM	network segment of CM: 2001:0db8:0001::/64
User-side of OLT	IP address of the gateway for the DHCP domain of CMs: 2001:0db8:0001::1/64; domain name: **docsis**
Network-side of OLT	Forwarding DHCP and broadband packets: ● VLAN ID: 2004 ● Port number: 0/4/0 ● IP address: 2001:0db8:0007::12/64 Forwarding CM management packets, multicast packets, and VoD packets: ● VLAN ID: 2005 ● Port number: 0/5/0 ● IP address: 2001:0db8:0008::13/64

Copyright © Huawei Technologies Co., Ltd.

Configuration Item	Data
Router	● IP address of the Layer 3 interface for forwarding DHCP and broadband packets: 2001:0db8:0007::6/64 ● IP address of the Layer 3 interface for forwarding CM management packets: 2001:0db8:0008::7/64
Server	● IP addresses of DHCP servers: – DHCP server allocating IP addresses for CMs: 2001:0db8:0006::8/64-2001:0db8:0006::9/64 – DHCP server allocating IP addresses for PCs: 2001:0db8:0006::10/64-2001:0db8:0006::11/64 ● IP addresses of the CM management system: 2001:0db8:0011::14/64-2001:0db8:0011::16/64

Procedure

Step 1 Create VLAN Layer 3 interfaces on the network side.

1. Create VLANs and add an uplink port to them, respectively.
   - VLAN 2004 used for forwarding DHCP packets is a smart VLAN. Add uplink port 0/4/0 to VLAN 2004.
   - VLAN 2005 used for forwarding CM management packets is a smart VLAN. Add uplink port 0/5/0 to VLAN 2005.

```
huawei(config)#vlan 2004 to 2005 smart
huawei(config)#port vlan 2004 0/4 0
huawei(config)#port vlan 2005 0/5 0
```

2. (Optional) Create native VLANs for Ethernet outbound ports.

   Packets between the OLT and its upper-layer router are forwarded at Layer 3 and no VLAN tag is required. The created native VLANs remove VLAN tags from the packets transmitted out of Ethernet ports.

```
huawei(config)#interface eth 0/4
huawei(config-if-eth-0/4)#native-vlan 0 vlan 2004    //The packets transmitted
out of port 0/4/0 are untagged.
huawei(config-if-eth-0/4)#quit
huawei(config)#interface eth 0/5
huawei(config-if-eth-0/5)#native-vlan 0 vlan 2005    //The packets transmitted
out of port 0/5/0 are untagged.
huawei(config-if-eth-0/5)#quit
```

3. Create VLAN Layer 3 interfaces.
   a. Create the Layer 3 interface of VLAN 2004, through which DHCP packets are forwarded.

```
huawei(config)#interface vlanif 2004
huawei(config-if-vlanif2004)#ipv6 address 2001:0db8:0007::12/64
huawei(config-if-vlanif2004)#quit
```

   b. Create the Layer 3 interface of VLAN 2005, through which CM management packets are forwarded.

Copyright © Huawei Technologies Co., Ltd.

```
huawei(config)#interface vlanif 2005
huawei(config-if-vlanif2005)#ipv6 address 2001:0db8:0008::13/64
huawei(config-if-vlanif2005)#quit
```

Step 2 Configure static routes for the communication between the OLT and its upper-layer devices.

```
huawei(config)#ipv6 route-static 2001:0db8:0006::/64 2001:0db8:0008::7/64     //CM
management packets are forwarded through the Layer 3 interface of VLAN 2005.
huawei(config)#ipv6 route-static 2001:0db8:0011::/64 2001:0db8:0007::6/64     //
DHCP packets are forwarded through the Layer 3 interface of VLAN 2004.
```

NOTE

Configure static routes on the router connected to the OLT. In addition, add the static routes to dynamic ones.

----End

Result

The OLT can communicate with its upper-layer devices. To check network connectivity between two devices, run the **ping ipv6** and **tracert ipv6** commands.

The configured static routes can be queried in an IPv6 routing table by running the **display ipv6 routing-table** command.

16.3.2.7 Configuring a Management Channel Between an OLT and an MA5633

This section describes how to configure a management channel between an optical line terminal (OLT) and a distributed cable modem termination system (D-CMTS). After the configuration, you can log in to the D-CMTS from the OLT and configure the D-CMTS.

Prerequisites

The MA5633 management policy is set to **stand-alone**. To do so, run the **sysman centralized-mgmt primary** command.

Data Plan

Item	Data	Remarks
OLT	GE port: 0/3/0	● Do not enable both the remote software commissioning using PON upstream transmission and the remote software commissioning using GE upstream transmission. ● Ensure that the database of a newly deployed D-CMTS is empty. Otherwise, the remote software commissioning using GE upstream transmission cannot be used. ● Only the network management parameters defined in SNMPv1 and SNMPv2 are supported.
Management VLAN and IP address of the D-CMTS	ID of the management VLAN: 8 Type of the management VLAN: smart Management IP address: 192.168.50.2/24	

Copyright © Huawei Technologies Co., Ltd.

Item	Data	Remarks
Management profile of the D-CMTS	ID: 64 Name: snmp-profile_64 SNMP version: SNMPv2c	● When the D-CMTS automatically obtains management parameters, it automatically generates a default route that can be restored. However, the default route may not be proper in service configuration. Therefore, you are advised to add a new route and delete the default one after the D-CMTS management channel is available. ● After the D-CMTS automatically obtains management parameters, the remote software commissioning function is automatically disabled if configurations are issued to the D-CMTS through the U2000. To modify the D-CMTS management parameters, remotely log in to the D-CMTS through the command line interface (CLI).

Procedure

Step 1 Configure a management channel between the OLT and the D-CMTS.

1. Configure the inband management VLAN and IP address of the OLT.

```
huawei(config)#vlan 8 smart
huawei(config)#port vlan 8 0/5 0
huawei(config)#interface vlanif 8
huawei(config-if-vlanif8)#ip address 192.168.50.1 24
huawei(config-if-vlanif8)#quit
```

2. Enable Network Admission Control (NAC) on the OLT.

```
huawei(config)#nac enable master 0/3 0
```

3. (Optional) Create an SNMP management profile.

   Perform this operation if the D-CMTS is managed through the U2000. Plan an SNMP management profile on the U2000 and D-CMTS before creating the profile.

```
huawei(config)#snmp-profile add profile-id 64 profile-name snmp-profile_64 v2c
public
private 192.168.50.55 30000 trapstatus
```

4. Configure D-CMTS management parameters on the OLT.

```
huawei(config)#nac config master 0/3/0 slave vlan 8 priority 6 ip-address
192.168.50.2 mask 255.255.255.0 gateway 192.168.50.1 snmp-profile-id 64
```

   Check whether the D-CMTS management parameters have been configured on the OLT.

```
huawei(config)#display nac configuration master
{ <cr>|frameid/slotid/portid<S><Length 1-255>|frameid/slotid<S><Length
```


Copyright © Huawei Technologies Co., Ltd.

```
1-15> }:

  Command:
          display nac configuration master

------------------------------------------------------------------------------
  Frame ID/Slot ID/Port ID :  0/3/0
  VLAN                     :  8
  VLAN priority            :  3
  IP address               :  192.168.50.2
  Mask                     :  255.255.255.0
  Gateway                  :  192.168.50.254
  Snmp-profile-id          :  64
  Snmp-profile-name        :  snmp-profile_64

------------------------------------------------------------------------------
Total: 1
```

Step 2 Check whether the management channel between the OLT and the D-CMTS is available.

Upon power-on, the D-CMTS exchanges data with the OLT to obtain the management parameters.

- Run the **ping** ***192.168.50.2*** command on the OLT to check whether the D-CMTS can communicate with the OLT. If the OLT can receive Internet Control Message Protocol (ICMP) ECHO-REPLY packets sent from the D-CMTS, the D-CMTS is connected to the OLT.
- Run the **telnet** command on the OLT to remotely log in to the ONU from the OLT to perform the configuration. The user name is root and the password is mduadmin.

----End

16.3.2.8 Configuring a Service Channel Between an OLT and a D-CMTS

Data Plan

Item	Data
L2VPN enterprise service	ID of the OLT VLAN (transparently transmitting D-CMTS packet tags): 200 ID of the D-CMTS VLAN: 200
Uplink ports	Port forwarding Dynamic Host Configuration Protocol (DHCP) and broadband packets: 0/4/0 Port forwarding cable modem (CM) management and VoD packets: 0/5/0

Procedure

- Configure a channel for the L2VPN enterprise service.
  1. Configure an L2VPN service VLAN (S-VLAN).

     The following configurations are used as an example to configure an S-VLAN:

     - S-VLAN ID: 200

Copyright © Huawei Technologies Co., Ltd.

- S-VLAN type: smart
- ID of the VLAN containing uplink port 0/4/0: 200 (S-VLAN ID)

```
huawei(config)#vlan 200 smart
huawei(config)#port vlan 200 0/4 0
```

2. Configure a service flow to receive and transparently transmit D-CMTS packets.

   The following configurations are used as an example to configure service flows:

   - Configuration of a service flow:
     - Service flow ID: 1
     - S-VLAN ID: 200
     - Customer VLAN (C-VLAN) ID: 200
   - Device where upstream and downstream packet rates are limited: D-CMTS

     In this case, use the default traffic profile with ID 6, which does not limit the rate of a service flow. To limit packet rates, run the **traffic table ip** command to create a traffic profile and bind it to the service flow.
   - C-VLAN and S-VLAN of the D-CMTS: same

   ```
   huawei(config)#service-port 1 vlan 200 eth 0/3/0 multi-service
   user-vlan 200 rx-cttr 6 tx-cttr 6
   ```

3. Configure the maximum number of dialup users allowed on a service port.

   For functions (such as, MAC address spoofing, anti-IP spoofing, anti-IPv6 spoofing, DHCP Proxy, IP Aware, IPoE single-MAC, VMAC DHCP aging, NS proxy response, ARP proxy response, DAD proxy, and DHCPv6 associated routes) depending on dialup operations performed by DHCP, DHCPv6, PPPoE, and SLAAC users, run this command to restrict the number of users allowed on each service port.

   ```
   huawei(config)#security user max-user-count service-port 1 2048
   huawei(config)#security user max-user-count service-port 2 2048
   ```

- Configure a CM management channel.

  1. Configure a service flow to receive and transparently transmit D-CMTS packets.

     The following configurations are used as an example to configure service flows:

     - Configuration of a service flow:
       - Service flow ID: 2
       - S-VLAN ID: 100
       - C-VLAN ID: 100
     - Device where upstream and downstream packet rates are limited: D-CMTS

       In this case, use the default traffic profile with ID 6, which does not limit the rate of a service flow. To limit packet rates, run the **traffic table ip** command to create a traffic profile and bind it to the service flow.
     - C-VLAN and S-VLAN of the D-CMTS: same

     ```
     huawei(config)#service-port 2 vlan 100 eth 0/3/0 multi-service
     user-vlan 100 rx-cttr 6 tx-cttr 6
     ```

  2. Configure the maximum number of dialup users allowed on a service port.

     ```
     huawei(config)#security user max-user-count service-port 2 2048
     ```


Copyright © Huawei Technologies Co., Ltd.

NOTE

- On IPv6 networks, run the **dhcpv6-option permit-forwarding port 0/3/0 enable** command to enable DHCPv6 Option forwarding on a specified port.
- If CPEs support IPv6 prefixes, run the **security bind-route-nd enable** command to enable associated routes and neighbor entries. Then, the OLT automatically generates the routing and neighbor entries of a DHCPv6 user based on the user information recorded when the user goes online. This prevents the need of manually configuring static routes and sending neighbor discovery (ND) packets to the user side, thereby improving system security.

----End

16.3.2.9 Configuring RF Port Parameters on an MA5633

Radio frequency (RF) port parameters define the frequency spectrum range for signal transmission and modulation mode. The configuration of RF port parameters implements data service transmission over cables.

Data Plan

Table 16-21 Data plan for RF port parameters

Item	Data
RF port	0/1/0
Upstream channels	● IDs: 1-4 ● Type: European standard (default channel type) ● ID of the upstream channel modulation profile: 1 (by default) ● Channel central frequency (MHz): 29.8, 42.60, 49.00, and 55.4
Downstream channels	● IDs: 1-16 ● Type: European standard (default channel type) ● Channel central frequency (MHz): 602.00, 610.00, 618.00, ..., and 722.00

Procedure

- Log in to and configure the ONU.

  You can remote log in to the ONU from the OLT to perform the configuration. The user name is **root** and the password is **mduadmin**.
- Customize RF port parameters in cable mode.
  1. Configure the frequency spectrum range and channel type.

     In this example, the channel is of the European type. To change the type to North American, run the **cable** command.
  2. Configure RF port parameters for upstream channels and activate the upstream channels.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
frequency and **channel-width**	A central frequency and a frequency bandwidth determine a frequency range, within which packets are transmitted. For example, the central frequency of a European channel is 55 MHz and the frequency bandwidth is 6400 kHz. Then the frequency range of the channel is 51.8-58.2 MHz.
modulation-profile	An upstream channel modulation profile defines parameters for processing the signals transmitted over the upstream channel. You do not need to configure an upstream channel modulation profile generally. Ports automatically bind to profile 1 by default.

The following configurations are used as an example to configure RF port parameters:

- Number of upstream channels: 4
- Frequency bandwidth of the channels: 3.2 MHz (default value)

```
huawei(config)#interface cable 0/1/0
huawei(config-if-cable-0/1/0)#cable upstream 1 frequency 29.8 enable
huawei(config-if-cable-0/1/0)#cable upstream 2 frequency 42.60 enable
huawei(config-if-cable-0/1/0)#cable upstream 3 frequency 49.00 enable
huawei(config-if-cable-0/1/0)#cable upstream 4 frequency 55.40 enable
```

3. Configure RF port parameters for downstream channels and activate the downstream channels.

Parameter	Description
modulation	A greater modulation mode value for downstream channels results in a higher channel bandwidth but weaker anti-interference capability. Therefore, configure the modulation mode based on site requirements. The default modulation mode is QAM256. This example uses the default setting.

The following configuration is used as an example to configure RF parameters for downstream channels: A total of 16 downstream channels have been purchased.

```
huawei(config-if-cable-0/1/0)#cable downstream 1 frequency 602.00 enable
huawei(config-if-cable-0/1/0)#cable downstream 2 frequency 610.00 enable
huawei(config-if-cable-0/1/0)#cable downstream 3 frequency 618.00 enable
huawei(config-if-cable-0/1/0)#cable downstream 4 frequency 626.00 enable
huawei(config-if-cable-0/1/0)#cable downstream 5 frequency 634.00 enable
huawei(config-if-cable-0/1/0)#cable downstream 6 frequency 642.00 enable
huawei(config-if-cable-0/1/0)#cable downstream 7 frequency 650.00 enable
```


Copyright © Huawei Technologies Co., Ltd.

```
huawei(config-if-cable-0/1/0)#cable downstream 8 frequency 658.00 enable
huawei(config-if-cable-0/1/0)#cable downstream 9 frequency 666.00 enable
huawei(config-if-cable-0/1/0)#cable downstream 10 frequency 674.00 enable
huawei(config-if-cable-0/1/0)#cable downstream 11 frequency 682.00 enable
huawei(config-if-cable-0/1/0)#cable downstream 12 frequency 690.00 enable
huawei(config-if-cable-0/1/0)#cable downstream 13 frequency 698.00 enable
huawei(config-if-cable-0/1/0)#cable downstream 14 frequency 706.00 enable
huawei(config-if-cable-0/1/0)#cable downstream 15 frequency 714.00 enable
huawei(config-if-cable-0/1/0)#cable downstream 16 frequency 722.00 enable
```

----End

Result

1. The transmit power of the downstream channels meets site requirements.

   Run the **display cable downstream** *frameid/slotid/portid* { **all** | *channel-id* } **status** command to check whether the RF port parameters meet site requirements.

2. The signal-to-noise (SNR) ratio of the upstream channels meets site requirements.

   Run the **display cable signal quality** [*frameid/slotid/portid* [**upstream** *channel-id*]] command to check whether the RF port parameters meet site requirements. A greater SNR ratio results in better signal quality. The recommended SNR ratio is greater than 30 dB.

16.3.2.10 Configuring the L2VPN Enterprise Service(on the CMC)

In the upstream direction, a cable modem (CM) connects to a distributed cable modem termination system (D-CMTS) through a cable. In the downstream direction, the CM connects to a switch to provide the L2VPN enterprise service to the users connected to the switch.

Context

An L2VPN S-VLAN can be configured through a CM configuration file or commands. Only one mode is used each time generally. If both modes are used, the S-VLAN configuration through commands preferentially takes effect on the system when the CM goes online.

- S-VLAN configuration through a CM configuration file: Run the **vlan** command to add a CM S-VLAN and run the **port vlan** command to add the uplink port for the CM to the S-VLAN. Then, run the **cable service-vlan** command to make the CM go online. The L2VPN S-VLAN is specified in the CM configuration file. When the CM goes online, the system obtains the L2VPN S-VLAN from the CM configuration file and automatically creates L2VPN service flows.
- S-VLAN configuration through commands: Manually configure the L2VPN S-VLAN on the system. For details, see the following procedure.

Data Plan

Table 16-22 Data plan for the L2VPN service

Item	Data
VLAN	ID of the L2VPN S-VLAN: 200; type of the VLAN: smart
Uplink port	0/0/1

Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Log in to and configure the ONU.

You can remote log in to the ONU from the OLT to perform the configuration. The user name is **root** and the password is **mduadmin**.

Step 2 Configure a CM management S-VLAN.

The ID of the CM management S-VLAN is 100 and the type of the VLAN is smart.

```
huawei(config)#vlan 100 smart
huawei(config)#port vlan 100 0/0 1
huawei(config)#cable service-vlan 100     //The CM S-VLAN identifies a CM service
flow. After the CM S-VLAN is configured, the D-CMTS automatically creates a service
flow when the CM goes online.
  Info: The new service VLAN will take effect after the CM is restarted, are you
 sure to modify? (y/n)[n]:y
```

Step 3 Create an L2VPN S-VLAN and add the uplink port to it.

The ID of the L2VPN S-VLAN is 200 and the type of the VLAN is smart. Uplink port 0/0/1 is added to S-VLAN 200.

When the L2VPN S-VLAN is configured through commands, the ID of the L2VPN VLAN is 200 for the CM with MAC address 0000-0000-1111 connected to port 0/1/0.

- To configure the L2VPN S-VLAN through a CM configuration file, run the following commands:
  ```
  huawei(config)#vlan 200 smart
  huawei(config)#port vlan 200 0/0 1
  ```
- To configure the L2VPN S-VLAN through commands, run the following commands:
  ```
  huawei(config)#vlan 200 smart
  huawei(config)#cable l2vpn dot1q 0/1/0 cm 0000-0000-1111 200
  huawei(config)#port vlan 200 0/0 1
  ```

----End

16.3.2.11 Verifying Services

A distributed cable modem termination system (D-CMTS) locates on an optical node when the D-CMTS functions as a standalone NE. To facilitate service verification, the D-CMTS supports multiple remote service verification methods, such as Dynamic Host Configuration Protocol (DHCP) dialup emulation tests. This allows commissioning and configuration engineers to remotely verify services. In addition, this section describes how to verify the L2VPN service on site.

Prerequisites

- The D-CMTS is properly connected to the upper-layer network.
- The DHCP server, Trivial File Transfer Protocol (TFTP) server, and softswitch or IP multimedia subsystem (IMS) have been configured.

Procedure

- Log in to and configure the ONU.

Copyright © Huawei Technologies Co., Ltd.

You can remote log in to the ONU from the OLT to perform the configuration. The user name is **root** and the password is **mduadmin**.

- Perform a DHCP dialup emulation test.

  In this test, a cable modem (CM) is emulated on the MA5633 to apply to the DHCP server for an IP address. This checks whether the MA5633 can communicate with the DHCP server and verifies CM DHCP configurations on the DHCP relay, proxy, and server.

  1. Run the **simulate dhcp start cm** *mac-address* [**option60** *option60*] command to start a DHCP dialup emulation test.

     NOTE

     You can run the **simulate dhcp stop** command to stop the DHCP emulation.

  2. Run the **display simulation dhcp** command to query the results of the DHCP dialup emulation test.
  3. Check whether the **User IP** has obtained an IP address.

- Check the CM status.

  Run the **display cable modem** command to query the CM status in **Status**.

```
huawei(config)#display cable modem  all

------------------------------------------------------------------------------
-
 Idx   MAC            IP              I/F          Status   Prim  Num Ver  DS
RX
                                                           SID   CPE
Power

------------------------------------------------------------------------------
-
 1     0023-ED6F-21A3 192.168.1.118   1/1/0/U4     ol-pt    1     0   D2.0
-

------------------------------------------------------------------------------
-
 Total:
1
 ol: 0, ol-ptd: 0, ol-pt: 1, ol-d: 0, wol: 0, wol-ptd: 0, wol-pt: 0, wol-d:
0,
pol: 0, pol-ptd: 0, pol-pt: 0, pol-d: 0, offline: 0, rej-m: 0, rej-pt: 0, rej-
o:
 0, init: 0, init-rc: 0, DHCP: 0, DHCP-O: 0, DHCP-R: 0, DHCP-C: 0, REG:
0
 Note: 1. Idx is the index of a
CM.
       2. The downstream received power is in the unit of
dBmV.
       3. In status, "ol" means online, "rej" means reject.
```

  The following table lists the CM status and handling suggestions.

CM Status	Description	Handling Suggestion
init	Indicates that the CM initialization ranging message is received.the CM initialization.	If a CM is always in the ranging state, the ranging fails. Then check radio frequency (RF) line indicators and detect line faults.

Copyright © Huawei Technologies Co., Ltd.

CM Status	Description	Handling Suggestion
init-rc	Indicates that the CM initialization ranging is complete.	No action is required. The ranging of the CM is complete.
DHCP	Indicates that the DHCP discovery from the CM is received.	If a CM initiates a DHCP request but does not obtain an IP address, check the DHCP server, routing between the OLT and the DHCP server, and DHCP server parameter settings.
● DHCP-O ● DHCP-R ● DHCP-C	● DHCP-O: indicates that the offer from the DHCP server is received. ● DHCP-R: indicates that the DHCP request from the CM is received. ● DHCP-C: indicates that the acknowledge from the DHCP server is received.	The DHCP server has assigned an IP address to the CM and sent configuration file name and IP address of the TFTP or ToD server to the CM using the Option 67 and Option 66 fields (the Option 67 field carries the configuration file name and the Option 66 field carries the IP address of the TFTP or ToD server). If the CM is always in the DHCP-C state, the CM fails to obtain the configuration file. Then check the TFTP server, routing between the OLT and the TFTP server, and TFTP server parameter settings.
REG	Indicates that a registration is started.	If the CM is always in the register state, the CM obtains an incorrect configuration file. Then change the configuration file.

Copyright © Huawei Technologies Co., Ltd.

CM Status	Description	Handling Suggestion
● ol ● ol-pt ● ol-ptd ● ol-d ● wol ● wol-pt ● wol-ptd ● wol-d ● pol ● pol-pt ● pol-ptd	● ol: indicates that the CM is online. (valid only for CMs complying with DOCSIS 2.0) ● ol-pt: indicates that the CM is online and passes the BPI authentication. (valid only for CMs complying with DOCSIS 2.0) ● ol-ptd: indicates that the CM is online and passes the BPI authentication, and NetAccessEnable is disabled. (valid only for CMs complying with DOCSIS 2.0) ● ol-d: indicates that the CM is online and NetAccessEnable is disabled. (valid only for CMs complying with DOCSIS 2.0) ● wol: indicates that the CM is online and all channels bound to the CM are available. (valid only for CMs complying with DOCSIS 3.0) ● wol-pt: indicates that the CM is online and passes the BPI authentication, and all channels bound to the CM are available. (valid only for CMs complying with DOCSIS 3.0) ● wol-ptd: indicates that the CM is online and passes the BPI authentication, NetAccessEnable is disabled, and all channels bound to the CM are available. (valid only for CMs complying with DOCSIS 3.0) ● wol-d: indicates that the CM is online, NetAccessEnable is disabled, and all channels bound to the CM are available. (valid only for CMs complying with DOCSIS 3.0) ● pol: indicates that the CM is online and some channels	No action is required. The status indicates that the CM has registered

Copyright © Huawei Technologies Co., Ltd.

CM Status	Description	Handling Suggestion
● pol-d	bound to the CM are available. (valid only for CMs complying with DOCSIS 3.0) ● pol-pt: indicates that the CM is online and passes the BPI authentication, and some channels bound to the CM are available. (valid only for CMs complying with DOCSIS 3.0) ● pol-ptd: indicates that the CM is online and passes the BPI authentication, NetAccessEnable is disabled, and some channels bound to the CM are available. (valid only for CMs complying with DOCSIS 3.0) ● pol-d: indicates that the CM is online, NetAccessEnable is disabled, and some channels bound to the CM are available. (valid only for CMs complying with DOCSIS 3.0)	with the OLT and can correctly transmit and receive services.
offline	Indicates the offline status.	If the CM is in the offline state, check the power status, noise, and channel frequency of the CM.
● rej-m ● rej-pt ● rej-o	● rej-m: indicates that the MIC verification fails. ● rej-pt: indicates that the BPI authentication fails. ● rej-o: indicates that the authentication reject due to other reasons.	If the CM is in the reject state, no service flow can be created. Then check the CM authentication and CM message integrity check (MIC), and check whether class of service (COS) parameters specified in the CM configuration file are supported by the OLT.

- Verify that the L2VPN service can be provisioned.
  After the CM is installed in the enterprise and the switch connected to the CM is commissioned, L2VPN service can be provisioned.

----End

16.3.3 WLAN Hotspot Radio Backhaul Service Networking

In wireless local area network (WLAN) hotspot radio backhaul service networking, an MA5633 connects to cable modems (CMs) through radio frequency (RF) ports. A CM connects to wireless access points (APs) to provide wireless fidelity (Wi-Fi) access for users.

Copyright © Huawei Technologies Co., Ltd.

Service Requirements

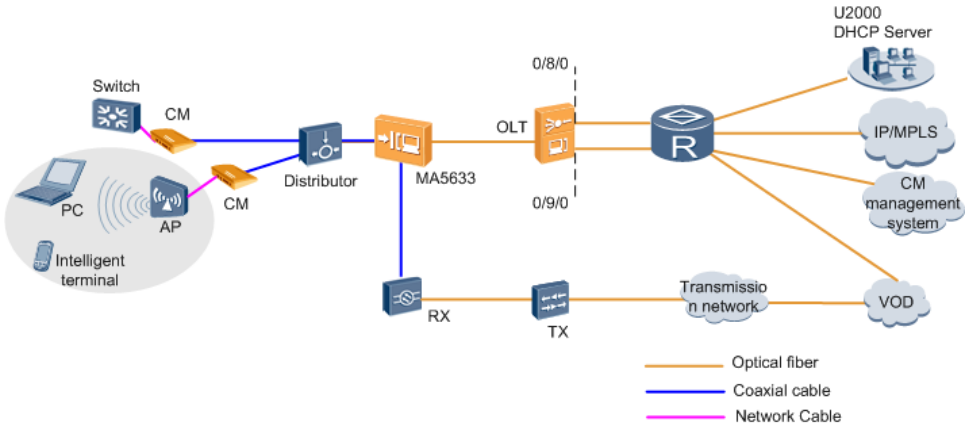
A network supplier needs to provide the Internet access service through Wi-Fi for a business area covered by APs.

Usage Scenario

As shown in **Figure 16-8**, an MA5633 is deployed on an optical node and cable modems (CMs) are deployed at shops. The CMs connect to radio frequency (RF) ports on the MA5633 through cables.

- A CM connects to wireless APs to provide the WLAN hotspot radio backhaul service. The wireless APs provide Wi-Fi access for users.
- Wi-Fi users access the Internet through Dynamic Host Configuration Protocol (DHCP) dialup.

Figure 16-8 WLAN hotspot radio backhaul service networking



Configuration

The method of configuring the wireless local area network (WLAN) hotspot radio backhaul service is the same as that of configuring the L2VPN enterprise service and therefore is not described in this section. For details, see **16.3.2.2 Configuration Process**.

16.4 Service Configuration on a D-CMTS That Works in GPON Access Mode on a Layer 3 Network

This section describes how to configure services, including home services, L2VPN enterprise service, and wireless local area network (WLAN) hotspot radio backhaul service, on a distributed cable modem termination system (D-CMTS) that works in GPON access mode on a Layer 3 network. The MA5603T equipped with the SCUV, GPBH, and SPUF boards is used as an example.

Control Board	SCUV

Copyright © Huawei Technologies Co., Ltd.

Service Board	GPMD: 0/3
SPU Board	SPUF: 0/4, 0/5

16.4.1 Home Service Networking

In home service networking, an MA5633 connects to cable modems (CMs) at user homes through radio frequency (RF) ports and provides home services for users, including the cable TV (CATV) service, Internet access service, VoD service, broadband TV (BTV) service, and PacketCable service. This section describes how to configure the optical line terminal (OLT) and the MA5633 to provision the home services.

NOTE

Configuration procedures are the same for IPv6 and IPv4 networks except in "Configure Dynamic Host Configuration Protocol (DHCP) relay" and "Configure a route". In addition, IPv6 does not support the function of configuring PacketCable dynamic voice services.

16.4.1.1 Service Requirements and Usage Scenario

Service Requirements

Users require the provisioning of the TV service, Internet access service, VoD service, broadband TV (BTV) service, and VoIP service. The TV service can be provisioned immediately after the distributed cable modem termination system (D-CMTS) hardware is connected. This section only describes how to configure the Internet access service, VoD service, BTV service, and VoIP service.

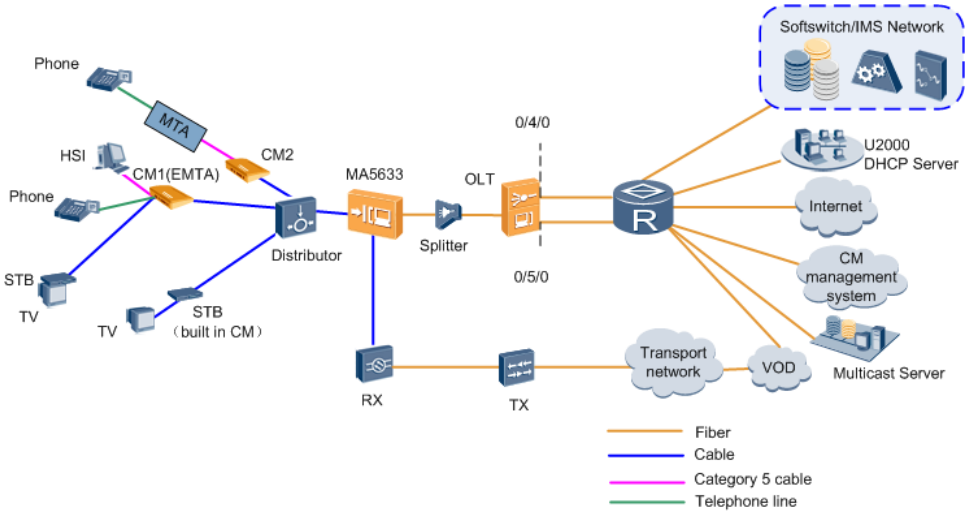
Usage Scenario

As shown in **Figure 16-9**, MA5633 is deployed on an optical node and cable modems (CMs) are deployed at user homes. The CMs connect to radio frequency (RF) ports on the MA5633 through cables.

- Port 1 on CM 1 connects to a PC for the Internet access service, port 2 connects to a phone set for the VoIP service, and the distributor connects to the STB for the VoD service. CM 1 supports embedded media terminal adapter (EMTA) functions and the voice users of CM 1 use PacketCable 1.x.
- CM 2 does not support EMTA functions and needs to connect to a media terminal adapter (MTA). The voice users of CM 2 use PacketCable Multimedia.
- Users access the Internet through Dynamic Host Configuration Protocol (DHCP) dialup.
- The IP addresses of the CM, STB, PC, and MTA are assigned by the DHCP server and in different network segments.

Copyright © Huawei Technologies Co., Ltd.

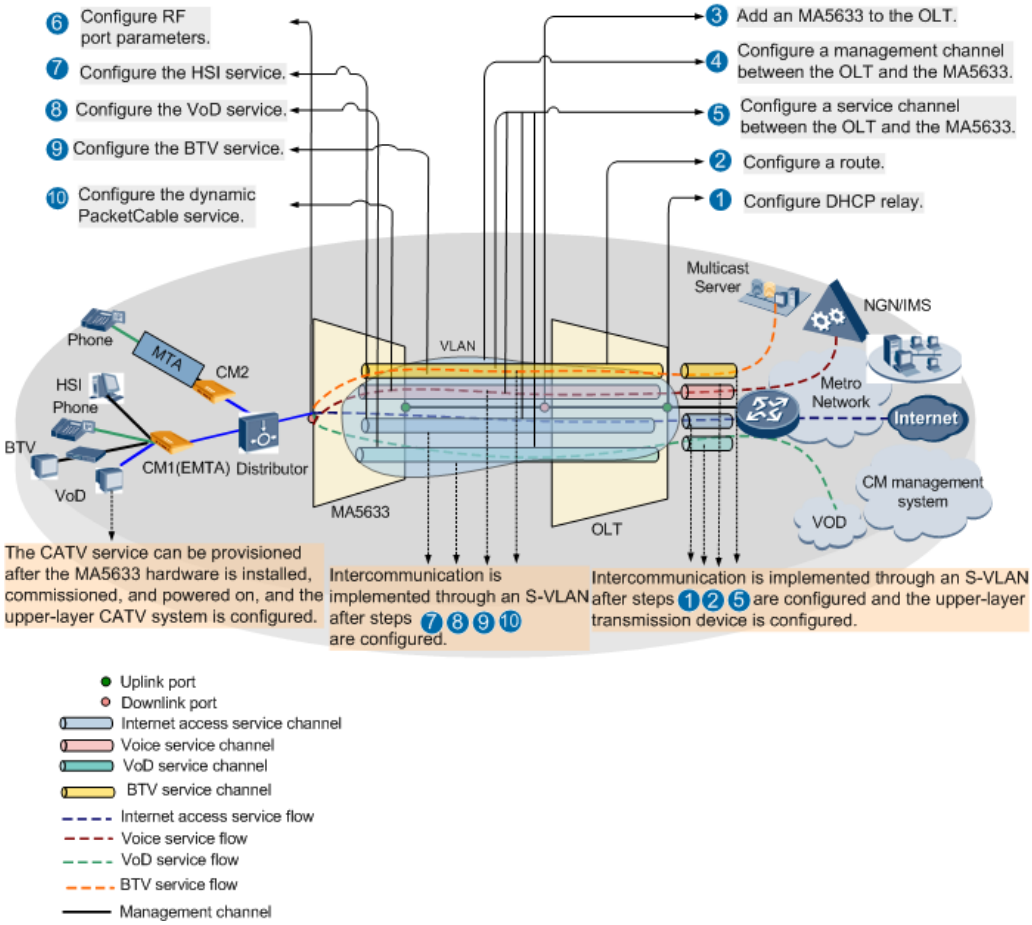
Figure 16-9 Home service networking



16.4.1.2 Configuration Process

Figure 16-10 shows the configuration roadmap for the home service networking.

Figure 16-10 Configuration roadmap for the home service networking



Copyright © Huawei Technologies Co., Ltd.

NOTE

Before logging in to the MA5633 to configure services on it, ensure that the MA5633 has been properly connected.

The following table describes the configuration steps.

Configuration Object	Step	Description
Optical line terminal (OLT)	● IPv4: **Configure Dynamic Host Configuration Protocol (DHCP) relay.** ● IPv6: **Configure Dynamic Host Configuration Protocol (DHCP) relay (IPv6).**	This section describes how to configure Dynamic Host Configuration Protocol (DHCP) relay so that cable modems (CMs) can obtain IP addresses in different network segments.
	● IPv4: **Configure a route.** ● IPv6: **Configure a route (IPv6).**	This section describes how to implement network communication by configuring a route in Layer 3 networking with an optical line terminal (OLT). Through the route, packets are forwarded at Layer 3 between the OLT and its upper-layer devices or servers.
	Add a D-CMTS to the OLT.	You can configure a distributed cable modem termination system (D-CMTS) only after adding it to an optical line terminal (OLT).
	Configure a management channel between the OLT and the D-CMTS.	This section describes how to configure a management channel between an optical line terminal (OLT) and a distributed cable modem termination system (D-CMTS). After the configuration, you can log in to the D-CMTS from the OLT and configure the D-CMTS.
	Configure a service channel between the OLT and the D-CMTS.	This section describes how to configure a service channel between an optical line terminal (OLT) and a distributed cable modem termination system (D-CMTS). After the configuration, the service channel forwards service packets on the D-CMTS based on the planned VLAN and forwarding policy.

Copyright © Huawei Technologies Co., Ltd.

Configuration Object	Step	Description
MA5633	**Configure radio frequency (RF) port parameters.**	Radio frequency (RF) port parameters define the frequency spectrum range for signal transmission and modulation mode. The configuration of RF port parameters implements data service transmission over cables.
	Configure the high-speed Internet (HSI) service.	None
	Configure the VoD service.	None
	Configure the broadband TV (BTV) service.	None
	Configure the dynamic PacketCable service.	None
	Verify the configured services.	A D-CMTS supports multiple remote service verification methods. This allows commissioning and configuration engineers to remotely verify services. 1. A DHCP dialup emulation test checks whether the D-CMTS can communicate with the DHCP server and verifies CM DHCP configurations on the DHCP relay, proxy, and server. 2. The status of a CM can be queried. Based on the information, you can determine whether the CM is online.

16.4.1.3 Configuring DHCP Relay

This section describes how to configure Dynamic Host Configuration Protocol (DHCP) relay so that cable modems (CMs) can obtain IP addresses in different network segments.

Prerequisites

The upper-layer router, DHCP server, and Trivial File Transfer Protocol (TFTP) server of an optical line terminal (OLT) have been configured.

Copyright © Huawei Technologies Co., Ltd.

Data Plan

Table 16-23 DHCP data plan for the OLT

Item	Data
VLAN	ID of the CM management S-VLAN: 100; type of the VLAN: smart
DHCP server group parameters	● IP address of the DHCP domain gateway for CMs: 10.10.224.1; domain name: docsis ● IP address of the DHCP domain gateway for media terminal adapters (MTAs): 10.100.224.1; domain name: pktc ● IP address of the DHCP domain gateway for paid PCs: 10.100.187.1; domain name: default ● IP address of the DHCP domain gateway for overdue PCs: 10.100.8.1; domain name: default ● IP address of the DHCP domain gateway for set top boxes (STB): 10.200.160.1; domain name: stb

Table 16-24 Data plan for the upper-layer devices of the OLT

Item	IP Address
Layer 3 interfaces connecting the router to the OLT	● Forwarding DHCP and broadband packets: 11.11.11.11 ● Forwarding CM management, VoD, and multicast packets: 11.11.12.11
IP addresses of DHCP servers	● DHCP server assigning IP addresses to CMs and MTAs: 192.168.10.10-192.168.10.11 ● DHCP server assigning IP addresses to PCs and STBs: 192.168.10.12-192.168.10.13
IP address of the TFTP server	192.168.5.10-192.168.5.13

Procedure

Step 1 Set the IP addresses of Layer 3 VLAN interfaces.

```
huawei(config)#vlan 100 smart
huawei(config)#interface vlanif 100
huawei(config-if-vlanif100)#arp proxy enable
huawei(config-if-vlanif100)#ip address 10.10.224.1 255.255.255.0 description
docsis     //Set the IP address of the DHCP domain gateway for CMs.
huawei(config-if-vlanif100)#ip address 10.100.224.1 255.255.255.0 sub description
pktc     //Set the IP address of the DHCP domain gateway for MTAs.
huawei(config-if-vlanif100)#ip address 10.200.160.1 255.255.255.0 sub description
stb     //Set the IP address of the DHCP domain gateway for STBs.
huawei(config-if-vlanif100)#ip address 10.100.187.1 255.255.255.0 sub description
default     //Set the IP address of the DHCP domain gateway for paid PCs.
```


Copyright © Huawei Technologies Co., Ltd.

```
huawei(config-if-vlanif100)#ip address 10.100.8.1 255.255.255.0 sub description
default      //Set the IP address of the DHCP domain gateway for overdue PCs.
huawei(config-if-vlanif100)#quit
```

Step 2 Configure the working mode of the DHCP relay to Layer 3 Option 60.

In DHCP Option 60 mode, a DHCP server group is selected according to the Option 60 domain name in DHCP packets. Users in this mode are identified by domain information of packets, which differentiates various service types in a VLAN. Ensure that the Option 60 domain name and the DHCP server group bound to the Option 60 domain name are configured beforehand.

```
huawei(config)#dhcp mode layer-3 Option60
  Several minutes may be required and no action can be taken during this period
  Are you sure to perform this operation? (y/n)[n]: y
```

Step 3 Enable the DHCP option82 feature.

The DHCP feature does not have any mechanism for authentication or security. Thus, the DHCP feature encounters many security problems when it is used in the network. To solve these problems, the DHCP option82 is introduced.

```
huawei(config)#dhcp option82 enable
```

Step 4 Set the IP addresses of the servers in a DHCP server group.

```
huawei(config)#dhcp-server 0 ip 192.168.10.10 192.168.10.11    //Configure DHCP
server group 0 to assign IP addresses to CMs and MTAs.
huawei(config)#dhcp-server 1 ip 192.168.10.12 192.168.10.13    //Configure DHCP
server group 1 to assign IP addresses to PCs and STBs.
```

Step 5 Create a DHCP Option 60 domain.

```
huawei(config)#dhcp domain default   //Create Option 60 domain name default for
PCs.
huawei(config-dhcp-domain-default)#dhcp-gateway learning enable   //Paid and
overdue PCs are in different network segments. Therefore, self-learning needs to be
enabled on OLT gateways.
huawei(config-dhcp-domain-default)#dhcp-server 1 vlan 100       //Bind DHCP server
group 1 to the DHCP domain where the PCs locate. After the configuration, the PCs
in the DHCP domain are corresponded to DHCP server group 1.
huawei(config-dhcp-domain-default)#quit
huawei(config)#dhcp domain docsis   //Create Option 60 domain name docsis for CMs.
huawei(config-dhcp-domain-docsis)#dhcp-server 0 vlan 100       //Bind DHCP server
group 0 to the DHCP domain where the CMs locate. After the configuration, the CMs
in the DHCP domain are corresponded to DHCP server group 0.
huawei(config-dhcp-domain-docsis)#quit
huawei(config)#dhcp domain pktc   //Create Option 60 domain name pktc for MTAs.
huawei(config-dhcp-domain-pktc)#dhcp-server 0 vlan 100       //Bind DHCP server
group 0 to the DHCP domain where the MTAs locate. After the configuration, the CMs
in the DHCP domain are corresponded to DHCP server group 0.
huawei(config-dhcp-domain-pktc)#quit
huawei(config)#dhcp domain stb   //Create Option 60 domain name stb for STBs.
huawei(config-dhcp-domain-stb)#dhcp-server 1 vlan 100     //Bind DHCP server group
1 to the DHCP domain where the STBs locate. After the configuration, the STBs in
the DHCP domain are corresponded to DHCP server group 1.
huawei(config-dhcp-domain-stb)#quit
```

Step 6 Set IP addresses of the gateways for the DHCP domain.

```
huawei(config)#interface vlanif 100
huawei(config-if-vlanif100)#dhcp domain default gateway 10.100.187.1
10.100.8.1    //Set the IP address of the gateway for the PC domain to 10.100.187.1
for paid PCs and to 10.100.8.1 for overdue PCs.
huawei(config-if-vlanif100)#dhcp domain docsis gateway 10.10.224.1    //Set the IP
address of the gateway for the CM domain to 10.10.224.1.
huawei(config-if-vlanif100)#dhcp domain pktc gateway 10.100.224.1    //Set the IP
address of the gateway for the MTA domain to 10.100.224.1.
huawei(config-if-vlanif100)#dhcp domain stb gateway 10.200.160.1    //Set the IP
```


Copyright © Huawei Technologies Co., Ltd.

```
address of the gateway for the STB domain to 10.200.160.1.
huawei(config-if-vlanif100)#quit
```

----End

16.4.1.4 Configuring a Route

This section describes how to implement network communication by configuring a route in Layer 3 networking with an optical line terminal (OLT). Through the route, packets are forwarded at Layer 3 between the OLT and its upper-layer devices or servers.

Prerequisites

The upper-layer router has been configured.

Data Plan

Table 16-25 Data plan for the Layer 3 interfaces on the network side

Item	IP Address
Layer 3 interfaces on the OLT network side	Forwarding Dynamic Host Configuration Protocol (DHCP) and broadband packets: ● VLAN ID: 2004 ● Port number: 0/4/0 ● IP address: 11.11.11.10/24 Forwarding cable modem (CM) management, VoD, COPS, and multicast packets: ● VLAN ID: 2005 ● Port number: 0/5/0 ● IP address: 11.11.12.10/24
Layer 3 interfaces connecting the router to the OLT	● Forwarding DHCP and broadband packets: 11.11.11.11 ● Forwarding CM management, VoD, COPS, and multicast packets: 11.11.12.11 ● COPS gateway IP address: 192.168.60.1
Upper-layer servers of the OLT	● DHCP servers: – DHCP server assigning IP addresses to CMs and media terminal adapters (MTAs): 192.168.10.10-192.168.10.11 – DHCP server assigning IP addresses to PCs and set top boxes (STBs): 192.168.10.12-192.168.10.13 ● CM management system, VoD server, and multicast server: 192.168.20.10-192.168.20.12 ● Softswitch or IP multimedia subsystem (IMS) server: 192.168.50.10

Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Create Layer 3 VLAN interfaces on the network side.

1. Create VLANs and configure their uplink ports.
   - VLAN 2004 is of the smart VLAN type and used for forwarding DHCP and broadband packets. Add uplink port 0/4/0 to VLAN 2004.
   - VLAN 2005 is of the smart VLAN type and used for forwarding CM management, VoD, and multicast packets. Add uplink port 0/5/0 to VLAN 2005.

   ```
   huawei(config)#vlan 2004 to 2005 smart
   huawei(config)#port vlan 2004 0/4 0
   huawei(config)#port vlan 2005 0/5 0
   ```

2. (Optional) Create native VLANs for Ethernet outbound ports.

   Packets between the OLT and its upper-layer router are assumed to be forwarded at Layer 3 and no VLAN information is required. The created native VLANs remove VLAN tags from the packets transmitted out of Ethernet ports.

   ```
   huawei(config)#interface eth 0/4
   huawei(config-if-eth-0/4)#native-vlan 0 vlan 2004    //Remove VLAN tags from
   the packets transmitted out of the 0/8/0 port.
   huawei(config-if-eth-0/4)#quit
   huawei(config)#interface eth 0/5
   huawei(config-if-eth-0/5)#native-vlan 0 vlan 2005    //Remove VLAN tags from
   the packets transmitted out of the 0/9/0 port.
   huawei(config-if-eth-0/5)#quit
   ```

3. Create Layer 3 VLAN interfaces.
   a. Create a Layer 3 interface for VLAN 2004, through which DHCP and broadband packets are forwarded.

      ```
      huawei(config)#interface vlanif 2004
      huawei(config-if-vlanif2004)#ip address 11.11.11.10 255.255.255.0
      huawei(config-if-vlanif2004)#quit
      ```

   b. Create a Layer 3 interface for VLAN 2005, through which CM management and VoD packets are forwarded.

      ```
      huawei(config)#interface vlanif 2005
      huawei(config-if-vlanif2005)#ip address 11.11.12.10 255.255.255.0
      huawei(config-if-vlanif2005)#quit
      ```

Step 2 Configure static routes to implement the communication between the OLT and its upper-layer devices.

```
huawei(config)#ip route-static 0.0.0.0 0.0.0.0 11.11.11.11     //Broadband packets
are forwarded through the Layer 3 interface of VLAN 2004.
huawei(config)#ip route-static 192.168.20.0 255.255.255.0 11.11.12.11     //CM
management, VoD, and multicast packets are forwarded through the Layer 3 interface
of VLAN 2005.
huawei(config)#ip route-static 192.168.10.0 255.255.255.0 11.11.11.11     //DHCP
packets are forwarded through the Layer 3 interface of VLAN 2004.
huawei(config)#ip route-static 192.168.50.0 255.255.255.0 11.11.12.11
```

NOTE

- The interconnected router must set static routes and add the routes to dynamic routes.

----End

Copyright © Huawei Technologies Co., Ltd.

Result

The OLT can communicate with its upper-layer devices. To check network connectivity between two devices, run the **ping** and **tracert** commands.

The configured static routes can be queried in an IPv4 routing table by running the **display ip routing-table** command.

16.4.1.5 Configuring DHCP Relay (IPv6)

This section describes how to configure DHCPv6 relay so that terminals can obtain IP addresses in different network segments.

Prerequisites

The upper-layer router, DHCP server server of an OLT have been configured.

Data Plan

Table 16-26 DHCP data plan

Configuration Item	Data
Terminal-side of CM	● network segment of CM: 2001:0db8:0001::/64 ● network segment of PCs with fees paid: 2001:0db8:0003::/64 ● network segment of overdue PCs: 2001:0db8:0004::/64
User-side of OLT	● IP address of the gateway for the DHCP domain of CMs: 2001:0db8:0001::1/64; domain name: **docsis** ● IP address of the gateway for the DHCP domain of PCs with fees paid: 2001:0db8:0003::3/64; domain name: **default** ● IP address of the gateway for the DHCP domain of overdue PCs: 2001:0db8:0004::4/64; domain name: **default**
Network-side of OLT	Forwarding DHCP and broadband packets: ● VLAN ID: 2004 ● Port number: 0/4/0 ● IP address: 2001:0db8:0007::12/64 Forwarding CM management packets, multicast packets, and VoD packets: ● VLAN ID: 2005 ● Port number: 0/5/0 ● IP address: 2001:0db8:0008::13/64
Router	● IP address of the Layer 3 interface for forwarding DHCP and broadband packets: 2001:0db8:0007::6/64 ● IP address of the Layer 3 interface for forwarding CM management packets: 2001:0db8:0008::7/64

Copyright © Huawei Technologies Co., Ltd.

Configuration Item	Data
Server	● IP addresses of DHCP servers: – DHCP server allocating IP addresses for CMs: 2001:0db8:0006::8/64-2001:0db8:0006::9/64 – DHCP server allocating IP addresses for PCs: 2001:0db8:0006::10/64-2001:0db8:0006::11/64 ● IP addresses of the CM management system: 2001:0db8:0011::14/64-2001:0db8:0011::16/64

Procedure

Step 1 Configure the IP address of the VLAN Layer 3 interface.

```
huawei(config)#ipv6      //Enable IPv6 packet forwarding.
huawei(config)#vlan 100
huawei(config)#interface vlanif 100
huawei(config-if-vlanif100)#ipv6 enable     //Enable IPv6 on ports.
huawei(config-if-vlanif100)#undo ipv6 nd ra halt      //enables a router to send
RA messages.
huawei(config-if-vlanif100)#ipv6 nd autoconfig managed-address-flag    //Configure
the state-based auto-configuration address flag bit. The host obtains an IPv6
address using the state-based automatic configuration.
huawei(config-if-vlanif100)#ipv6 address 2001:0db8:0001::1/64     //Configure the
IP address of the gateway for the DHCP domain of CMs.
huawei(config-if-vlanif100)#ipv6 address 2001:0db8:0003::3/64     //Configure the
IP address of the gateway for the DHCP domain of PCs with fees paid.
huawei(config-if-vlanif100)#ipv6 address 2001:0db8:0004::4/64     //Configure the
IP address of the gateway for the DHCP domain of overdue PCs.
huawei(config-if-vlanif100)#quit
```

Step 2 Enable duplicate address detect (DAD) proxy, which prevents repeated link local addresses (LLAs) on the user side.

After receiving a DAD packet sent from the user side with destination IP address LLA, the OLT with DAD proxy enabled checks user online information based on the destination IP address and VLAN. If a user with the same IP address in the VLAN has been online, the OLT makes a response and prohibits the new user from going online. Otherwise, the OLT does not make a response.

```
huawei(config)#ipv6 dad proxy enable
huawei(config)#vlan service-profile profile-id 10
huawei(config)#vlan bind service-profile 100 profile-id 10
huawei(config-vlan-srvprof-10)#ipv6 dad proxy enable     //DAD proxy takes effect
after it is enabled at system level and VLAN service profile level.
```

Step 3 Configure the working mode of DHCP relay to Layer 3 Option 16.

Option 16 is an option with code 16 in DHCPv6 packets, which identifies terminal types. In DHCPv6 Option 16 mode, packets select a DHCPv6 server based on the Option 16 domain. Therefore, in DHCPv6 Option 16 mode, packets select a DHCPv6 server based on terminal types.

```
huawei(config)#dhcpv6 mode layer-3 option16
  Several minutes may be required and no action can be taken during this period
  Are you sure to perform this operation? (y/n)[n]: y
```

Step 4 Configure the IP addresses of the servers in a DHCP server group.

```
huawei(config)#dhcpv6-server 0 ipv6 2001:0db8:0006::8/64 2001:0db8:0006::9/64    //
Configure DHCP server group 0 to allocate IP addresses for CMs.
```


Copyright © Huawei Technologies Co., Ltd.

```
huawei(config)#dhcpv6-server 1 ipv6 2001:0db8:0006::10/64
2001:0db8:0006::11/64    //Configure DHCP server group 1 to allocate IP addresses
for PCs.
```

Step 5 Create DHCP Option 16 domains.

```
huawei(config)#dhcp domain default   //Create Option 16 domain default for PCs.
huawei(config-dhcp-domain-default)#dhcpv6-gateway learning enable   //PCs require
different IP address segments based on fee payment state. Therefore, automatic
gateway learning must be enabled on the OLT.
huawei(config-dhcp-domain-default)#dhcpv6-server 1 vlan 100        /Bind DHCP
server group 1 to the DHCP domain of PCs. After the configuration, the PCs in this
DHCP domain are mapped to DHCP server group 1.
huawei(config-dhcp-domain-default)#quit
huawei(config)#dhcp domain docsis   //Create Option 16 domain docsis for CMs.
huawei(config-dhcp-domain-docsis)#dhcpv6-server 0 vlan 100      //Bind DHCP server
group 0 to the DHCP domain of CMs. After the configuration, the CMs in this DHCP
domain are mapped to DHCP server group 0.
huawei(config-dhcp-domain-docsis)#quit
```

Step 6 Configure the IP addresses of the gateways for DHCP domains.

```
huawei(config)#interface vlanif 100
huawei(config-if-vlanif100)#dhcp domain default gateway ipv6 2001:0db8:0003::3/64
2001:0db8:0004::4/64    //Configure IP addresses of the gateways for the DHCP
domain of PCs, including the IP address of the gateway for the PCs with fees paid
and the IP address of the gateway for overdue PCs.
huawei(config-if-vlanif100)#dhcp domain docsis gateway ipv6
2001:0db8:0001::1/64    //Configure the IP address of the gateway for the DHCP
domain of CMs.

huawei(config-if-vlanif100)#quit
```

----End

16.4.1.6 Configuring a Route (IPv6)

This section describes how to implement network communication by configuring a route in Layer 3 networking with an OLT. Through the route, the OLT can forward packets at Layer 3 between the OLT and its upper-layer devices or servers.

Prerequisites

The upper-layer router of the OLT has been configured.

Data Plan

Table 16-27 DHCP data plan

Configuration Item	Data
Terminal-side of CM	● network segment of CM: 2001:0db8:0001::/64 ● network segment of PCs with fees paid: 2001:0db8:0003::/64 ● network segment of overdue PCs: 2001:0db8:0004::/64

Copyright © Huawei Technologies Co., Ltd.

Configuration Item	Data
User-side of OLT	● IP address of the gateway for the DHCP domain of CMs: 2001:0db8:0001::1/64; domain name: **docsis** ● IP address of the gateway for the DHCP domain of PCs with fees paid: 2001:0db8:0003::3/64; domain name: **default** ● IP address of the gateway for the DHCP domain of overdue PCs: 2001:0db8:0004::4/64; domain name: **default**
Network-side of OLT	Forwarding DHCP and broadband packets: ● VLAN ID: 2004 ● Port number: 0/4/0 ● IP address: 2001:0db8:0007::12/64 Forwarding CM management packets, multicast packets, and VoD packets: ● VLAN ID: 2005 ● Port number: 0/5/0 ● IP address: 2001:0db8:0008::13/64
Router	● IP address of the Layer 3 interface for forwarding DHCP and broadband packets: 2001:0db8:0007::6/64 ● IP address of the Layer 3 interface for forwarding CM management packets: 2001:0db8:0008::7/64
Server	● IP addresses of DHCP servers: – DHCP server allocating IP addresses for CMs: 2001:0db8:0006::8/64-2001:0db8:0006::9/64 – DHCP server allocating IP addresses for PCs: 2001:0db8:0006::10/64-2001:0db8:0006::11/64 ● IP addresses of the CM management system: 2001:0db8:0011::14/64-2001:0db8:0011::16/64

Procedure

Step 1 Create VLAN Layer 3 interfaces on the network side.

1. Create VLANs and add an uplink port to them, respectively.
   - VLAN 2004 used for forwarding DHCP and broadband packets is a smart VLAN. Add uplink port 0/4/0 to VLAN 2004.
   - VLAN 2005 used for forwarding CM management packets, multicast packets, and VoD packets is a smart VLAN. Add uplink port 0/5/0 to VLAN 2005.

```
huawei(config)#vlan 2004 to 2005 smart
huawei(config)#port vlan 2004 0/4 0
huawei(config)#port vlan 2005 0/5 0
```

2. (Optional) Create native VLANs for Ethernet outbound ports.

Copyright © Huawei Technologies Co., Ltd.

Packets between the OLT and its upper-layer router are forwarded at Layer 3 and no VLAN tag is required. The created native VLANs remove VLAN tags from the packets transmitted out of Ethernet ports.

```
huawei(config)#interface eth 0/4
huawei(config-if-eth-0/4)#native-vlan 0 vlan 2004    //The packets transmitted
out of port 0/4/0 are untagged.
huawei(config-if-eth-0/4)#quit
huawei(config)#interface eth 0/5
huawei(config-if-eth-0/5)#native-vlan 0 vlan 2005    //The packets transmitted
out of port 0/5/0 are untagged.
huawei(config-if-eth-0/5)#quit
```

3. Create VLAN Layer 3 interfaces.

   a. Create the Layer 3 interface of VLAN 2004, through which DHCP and broadband packets are forwarded.

   ```
   huawei(config)#interface vlanif 2004
   huawei(config-if-vlanif2004)#ipv6 address 2001:0db8:0007::12/64
   huawei(config-if-vlanif2004)#quit
   ```

   b. Create the Layer 3 interface of VLAN 2005, through which CM management packets, multicast packets, and VoD packets are forwarded.

   ```
   huawei(config)#interface vlanif 2005
   huawei(config-if-vlanif2005)#ipv6 address 2001:0db8:0008::13/64
   huawei(config-if-vlanif2005)#quit
   ```

Step 2 Configure static routes for the communication between the OLT and its upper-layer devices.

```
huawei(config)#ipv6 route-static ::/0 2001:0db8:0007::6/64     //Broadband packets
are forwarded through the Layer 3 interface of VLAN 2004.
huawei(config)#ipv6 route-static 2001:0db8:0011::/64 2001:0db8:0008::7/64     //CM
management packets are forwarded through the Layer 3 interface of VLAN 2005.
huawei(config)#ipv6 route-static 2001:0db8:0006::/64 2001:0db8:0007::6/64     //
DHCP packets are forwarded through the Layer 3 interface of VLAN 2004.
```

NOTE

Configure static routes on the router connected to the OLT. In addition, add the static routes to dynamic ones.

----End

Result

The OLT can communicate with its upper-layer devices. To check network connectivity between two devices, run the **ping ipv6** and **tracert ipv6** commands.

The configured static routes can be queried in an IPv6 routing table by running the **display ipv6 routing-table** command.

16.4.1.7 Adding a D-CMTS to an OLT

You can configure a distributed cable modem termination system (D-CMTS) only after adding it to an optical line terminal (OLT).

Prerequisites

The MA5633 management policy is set to **stand-alone**. To do so, run the **sysman centralized-mgmt primary** command.

Copyright © Huawei Technologies Co., Ltd.

Context

- When adding a D-CMTS to an OLT, bind the following profiles to the D-CMTS: dynamic bandwidth allocation (DBA) profile, line profile, and alarm profile. For details about the functions and configuration method of each profile, see **Table 16-28**.

Table 16-28 D-CMTS profiles

Profile	Function	Command
DBA profile	Describes GPON traffic parameters. A transmission container (T-CONT) is bound to a DBA profile for dynamic bandwidth allocation. This improves the upstream bandwidth usage.	Command for querying a DBA profile: **display dba-profile** Command for adding a DBA profile: **dba-profile add**
Line profile	Describes the binding between a T-CONT and a DBA profile, quality of service (QoS) mode of a service flow, and mapping from a GEM port to D-CMTS services.	Command for querying a line profile: **display ont-lineprofile** Command for adding a line profile: **ont-lineprofile**
Alarm profile	Contains a series of alarm thresholds for measuring and monitoring the performance of activated D-CMTS lines.	Command for querying an alarm profile: **display gpon alarm-profile** Command for adding an alarm profile: **gpon alarm-profile add**

- Add a D-CMTS using either of the methods listed in the following table based on site requirements.

Method	Usage Scenario	Command
Add a D-CMTS in offline mode.	You have obtained the password or serial number (SN) of the D-CMTS.	Run the **ont add** command to add the D-CMTS to an OLT.
Add an online D-CMTS and confirm the automatically discovered D-CMTS.	You do not know the password or SN of the D-CMTS.	In GPON mode, run the **port ont-auto-find** command to enable the D-CMTS automatic discovery function on GPON ports. Then run the **ont confirm** command to add the D-CMTS.

Copyright © Huawei Technologies Co., Ltd.

Data Plan

Table 16-29 Key data plan

Item	Data
DBA profile	Profile name: PrivateLine Type: type4 Maximum bandwidth: 1000 Mbit/s
Line profile	Profile ID: 10, bound to DBA profile **PrivateLine** GPON encapsulation mode (GEM) port IDs: 0 and 1 T-CONT ID: 5
Networking data	Port: 0/3/1 D-CMTS ID: 1 D-CMTS authentication mode: SN D-CMTS SN: 48575443E6D8B541 Management VLAN: 8 Service VLAN: 100 Common open policy service (COPS) connection VLAN: 1000

Procedure

Step 1 Configure D-CMTS profiles.

D-CMTS profiles include a DBA profile, a line profile, and an alarm profile.

1. Configure a DBA profile.

   Run the **display dba-profile** command to query DBA profiles existing in the system. If the existingDBA profiles do not meet service requirements, run the **dba-profile add** command to add a DBA profile.

   ```
   huawei(config)#dba-profile add profile-name PrivateLine type4 max 1000000
   ```

2. Configure a line profile.

   Add line profile 10 and bind T-CONT 5 to DBA profile **PrivateLine**. In this way, the T-CONT provides flexible DBA solutions based on the configurations in the DBA profile.

   ```
   huawei(config)#ont-lineprofile gpon profile-id 10
   huawei(config-gpon-lineprofile-10)#tcont 5 dba-profile-name PrivateLine
   ```

   The following configurations are used as an example to add a line profile:

   - Index of the GEM port for carrying management service flows: 0
   - Index of the GEM port for carrying high-speed Internet (HSI) and VoD service flows: 1
   - ID of the T-CONT that GEM ports 0 and 1 are bound: 5
   - QoS mode: priority-queue (default)

Copyright © Huawei Technologies Co., Ltd.

- Queue priority of GEM ports 0 and 1: 3, 1

  NOTE

  When the QoS mode is PQ, the default queue priority is 0.

  huawei(config-gpon-lineprofile-10)#**gem add 0 eth tcont 5 priority-queue 3**

  huawei(config-gpon-lineprofile-10)#**gem add 1 eth tcont 5 priority-queue 1**

- Mode of the mapping from the GEM port to D-CMTS services: VLAN (default)
- Index of the GEM port to which the management service flows in VLAN 8 are mapped: 0
- Index of the GEM port to which the service flows in VLAN 100 are mapped: 1
- Index of the GEM port to which the service flows in COPS connection VLAN 1000 are mapped: 2

```
huawei(config-gpon-lineprofile-10)#mapping-mode vlan
huawei(config-gpon-lineprofile-10)#gem mapping 0 0 vlan 8
huawei(config-gpon-lineprofile-10)#gem mapping 1 1 vlan 100
huawei(config-gpon-lineprofile-10)#gem mapping 1 2 vlan 1000
```

Run the **commit** command to make the configured parameters take effect.

```
huawei(config-gpon-lineprofile-10)#commit
huawei(config-gpon-lineprofile-10)#quit
```

(Optional) Configure an alarm profile.

- The ID of the default GPON alarm profile is 1. In this profile, the thresholds for all alarm parameters in the default alarm profile are 0, which indicates that no alarm is generated.
- This section uses the default alarm profile and therefore the alarm profile does not need to be configured.
- To add an alarm profile for monitoring the performance of activated D-CMTS lines, run the **gpon alarm-profile add** command.

Step 2 Add a D-CMTS to an OLT.

The D-CMTS connects to a GPON port on the OLT through an optical fiber. You can configure the D-CMTS only after adding it to the OLT.

1. Add a D-CMTS.

   The following configurations are used as an example to add a D-CMTS: The management mode is SNMP; the ID of the line profile bound to the D-CMTS is 10.

   To add a D-CTMS in offline mode, do as follows:

```
huawei(config)#interface gpon 0/3
huawei(config-if-gpon-0/3)#ont add 1 1 sn-auth 48575443E6D8B541 snmp ont-
lineprofile-id
 10 desc MA5633_0/3/1/1_lineprofile10
```

   To automatically find a D-CMTS, do as follows:

```
huawei(config)#interface gpon 0/3
huawei(config-if-gpon-0/3)#port 1 ont-auto-find enable
huawei(config-if-gpon-0/3)#display ont autofind 1
   //This command displays the information about all automatically discovered
D-CMTSs that are connected to the GPON port through an optical splitter.

   ------------------------------------------------------------
   Number              : 1
   F/S/P               : 0/3/1
   Ont SN              : 48575443E6D8B541
   Password            : 0x30303030303030303030(0000000000)
   Loid                : 00000000000000000000000
```


Copyright © Huawei Technologies Co., Ltd.

```
   Checkcode           : 000000000000
   VendorID            : HWTC
   Ont Version         : MA5633 VER.A
   Ont SoftwareVersion : V8R313 C10
   Ont EquipmentID     : 5633
   Ont autofind time   : 2013-09-25 20:42:45+08:00
   ----------------------------------------------------------
huawei(config-if-gpon-0/3)#ont confirm 1 ontid 1 sn-auth 48575443E6D8B541 snmp
ont-lineprofile-id
 10 desc MA5633_0/3/1/1_lineprofile10
```

NOTE

If multiple D-CMTSs of the same type are connected to a port and the same line or service profile is bound to the D-CMTSs, add these D-CMTSs in batches by confirming the automatically discovered D-CMTSs in batches. This simplifies operations and improves configuration efficiency. To do so, change the preceding command huawei(config-if-gpon-0/3)#**ont confirm 1 ontid 1 sn-auth 48575443E6D8B541 snmp ont-lineprofile-id 10 desc MA5633_0/3/1/1_lineprofile10** to huawei(config-if-gpon-0/3)#**ont confirm 1 all sn-auth snmp ont-lineprofile-id 10 desc MA5633_0/3/1_lineprofile10**.

----End

Result

The D-CMTS is online.

After adding the D-CMTS, run the **display ont info** command to query the D-CMTS status. Ensure that **Control flag** is **active**, **Run State** is **online**, and **Config state** is **normal**.

```
huawei(config-if-gpon-0/3)#display ont info 1 1
  ------------------------------------------------------------------------
  F/S/P                : 0/3/1
  ONT-ID               : 1
  Control flag         : active    //The D-CMTS has been activated.
  Run state            : online    //The D-CMTS has been online.
  Config state         : normal    //The D-CMTS has been configured.
...//The following terminal display is omitted.
```

Follow-up Procedure

If the D-CMTS malfunctions, follow the troubleshooting suggestions listed in the following table to rectify faults.

D-CMTS Status	Troubleshooting Suggestion
The **Control flag** of the D-CMTS is **deactivated**.	In GPON port mode, run the **ont activate** command to activate the D-CMTS.
The D-CMTS is offline (**Run state** displayed as **offline**).	The physical line may be disconnected, or the optical module may be damaged. Rectify the fault by checking line connection and the hardware.
The D-CMTS fails to be configured (**Config state** displayed as **failed**)	The possible cause is that the D-CMTS cannot support the configured D-CMTS capability set. In this case, run the **display ont failed-configuration** command to query the failed configuration items and failure causes. Then rectify the fault accordingly.

Copyright © Huawei Technologies Co., Ltd.

16.4.1.8 Configuring a Management Channel Between an OLT and a D-CMTS

This section describes how to configure a management channel between an optical line terminal (OLT) and a distributed cable modem termination system (D-CMTS). After the configuration, you can log in to the D-CMTS from the OLT and configure the D-CMTS.

Data Plan

Item	Data	Remarks
Management VLAN and IP address of the OLT	ID of the management VLAN: 8 Type of the management VLAN: smart Management IP address: 192.168.50.1/24	To remotely log in to the D-CMTS from the OLT for configuration, ensure that the management VLAN of the OLT is the same as that of the D-CMTS and that the management IP address of the OLT is in the same network segment as that of the D-CMTS.
Management VLAN and IP address of the D-CMTS	ID of the management VLAN: 8 Type of the management VLAN: smart Management IP address: 192.168.50.2/24	

Procedure

Step 1 Configure a management channel between the OLT and the D-CMTS.

NOTE

Perform this operation only when the OLT remotely manages the D-CMTS through SNMP.

1. Set the inband management VLAN and IP address of the OLT.

   To remotely log in to the D-CMTS for configuration, set the inband management VLANs and IP addresses of the OLT and the D-CMTS on the OLT.

   ```
   huawei(config)#vlan 8 smart
   huawei(config)#port vlan 8 0/5 0
   huawei(config)#interface vlanif 8
   huawei(config-if-vlanif8)#ip address 192.168.50.1 24
   huawei(config-if-vlanif8)#quit
   ```

2. Set the inband management VLAN and IP address of the D-CMTS.

   Set the static IP address of the D-CMTS to 192.168.50.2/24, the IP address of the gateway to 192.168.50.1, and the ID of the management VLAN to 8 (the same as the management VLAN of the OLT).

   ```
   huawei(config)#interface gpon 0/3
   huawei(config-if-gpon-0/3)#ont ipconfig 1 1 static ip-address 192.168.50.2
   mask 255.255.255.0 gateway
       192.168.50.1 vlan 8
   huawei(config-if-gpon-0/3)#quit
   ```

3. Configure an inband management service flow.

   The following configurations are used as an example to configure an inband management service flow:

Copyright © Huawei Technologies Co., Ltd.

- Configuration of the service flow:
  - ID of the management service flow: 0
  - ID of the management VLAN: 8
  - ID of the GPON encapsulation mode (GEM) port: 0
  - ID of the customer VLAN (C-VLAN): 8
- Device where upstream and downstream packet rates are limited: D-CMTS

  In this case, use the default traffic profile with ID 6, which does not limit the rate of a service flow. To limit packet rates, run the **traffic table ip** command to create a traffic profile and bind it to the service flow.

```
huawei(config)#service-port 0 vlan 8 gpon 0/3/1 ont 1 gemport 0 multi-service
user-vlan 8 rx-cttr 6 tx-cttr 6
```

NOTE

- On IPv6 networks, run the **dhcpv6-option permit-forwarding port 0/3/0 enable** command to enable DHCPv6 Option forwarding on a specified port.
- If CPEs support IPv6 prefixes, run the **security bind-route-nd enable** command to enable associated routes and neighbor entries. Then, the OLT automatically generates the routing and neighbor entries of a DHCPv6 user based on the user information recorded when the user goes online. This prevents the need of manually configuring static routes and sending neighbor discovery (ND) packets to the user side, thereby improving system security.

Step 2 Check whether the management channel between the OLT and the D-CMTS is available.

- Run the **ping** ***192.168.50.1*** command on the OLT to check whether the D-CMTS can communicate with the OLT. If the OLT can receive Internet Control Message Protocol (ICMP) ECHO-REPLY packets sent from the D-CMTS, the D-CMTS is connected to the OLT.
- Run the **telnet** command on the OLT to remotely log in to the ONU from the OLT to perform the configuration. The user name is root and the password is mduadmin.

----End

16.4.1.9 Configuring a Service Channel Between an OLT and a D-CMTS

Data Plan

Item	Data
High-speed Internet (HSI), VoD, broadband TV (BTV), or dynamic PacketCable service	ID of the OLT VLAN (transparently transmitting D-CMTS packet tags): 100 ID of the D-CMTS VLAN: 100 ID of the common open policy service (COPS) connection VLAN: 1000

Procedure

- Configure a channel for a home service.
  1. Configure service flows to receive and transparently transmit D-CMTS packets.

     The following configurations are used as an example to configure service flows:

Copyright © Huawei Technologies Co., Ltd.

- Configuration of a service flow:
  - Service flow ID: 1
  - S-VLAN ID: 100
  - Customer VLAN (C-VLAN) ID: 100
- Configuration of a COPS connection service flow:
  - Service flow ID: 2
  - VLAN (shared with the S-VLAN) ID: 100
  - C-VLAN ID: 1000
- Device where upstream and downstream packet rates are limited: D-CMTS

  In this case, use the default traffic profile with ID 6, which does not limit the rate of a service flow. To limit packet rates, run the **traffic table ip** command to create a traffic profile and bind it to the service flow.
- C-VLAN and S-VLAN of the D-CMTS: same

```
huawei(config)#service-port 1 vlan 100 gpon 0/3/1 ont 1 gemport 1 multi-service
user-vlan 100 rx-cttr 6 tx-cttr 6
huawei(config)#service-port 2 vlan 100 gpon 0/3/1 ont 1 gemport 1 multi-service
user-vlan 1000 rx-cttr 6 tx-cttr 6
```

NOTE

- On IPv6 networks, run the **dhcpv6-option permit-forwarding port 0/3/0 enable** command to enable DHCPv6 Option forwarding on a specified port.
- If CPEs support IPv6 prefixes, run the **security bind-route-nd enable** command to enable associated routes and neighbor entries. Then, the OLT automatically generates the routing and neighbor entries of a DHCPv6 user based on the user information recorded when the user goes online. This prevents the need of manually configuring static routes and sending neighbor discovery (ND) packets to the user side, thereby improving system security.

2. Configure the maximum number of dialup users allowed on a service port.

   For functions (such as, MAC address spoofing, anti-IP spoofing, anti-IPv6 spoofing, DHCP Proxy, IP Aware, IPoE single-MAC, VMAC DHCP aging, NS proxy response, ARP proxy response, DAD proxy, and DHCPv6 associated routes) depending on dialup operations performed by DHCP, DHCPv6, PPPoE, and SLAAC users, run this command to restrict the number of users allowed on each service port.

   ```
   huawei(config)#security user max-user-count service-port 1 2048
   huawei(config)#security user max-user-count service-port 2 2048
   ```

3. Configure multicast cascading port 0/3/1.

   ```
   huawei(config)#btv
   huawei(config-btv)#igmp cascade-port 0/3/1 ontid 1 gemport-index 1
   huawei(config-btv)#quit
   ```

4. Configure the Internet Group Management Protocol (IGMP) version to IGMPv3.

   ```
   huawei(config)#multicast-vlan 100
   huawei(config-mvlan100)#igmp version v3
   ```

5. Configure the multicast uplink port to 0/5/0.

   ```
   huawei(config-mvlan100)#igmp uplink-port 0/5/0
   ```

6. Configure a multicast program generation mode.

   For the D-CMTS, the multicast programs are dynamically generated.

Copyright © Huawei Technologies Co., Ltd.

```
huawei(config-mvlan100)#igmp mode off
  Are you sure to close IGMP? (y/n)[n]:y
huawei(config-mvlan100)#igmp match mode disable
```

7. Configure the IGMP mode to IGMP proxy.

```
huawei(config-mvlan100)#igmp mode proxy
  Are you sure to change IGMP mode?(y/n)[n]:y
huawei(config-mvlan100)#quit
```

----End

16.4.1.10 Configuring RF Port Parameters on an MA5633

Radio frequency (RF) port parameters define the frequency spectrum range for signal transmission and modulation mode. The configuration of RF port parameters implements data service transmission over cables.

Data Plan

Table 16-30 Data plan for RF port parameters

Item	Data
RF port	0/1/0
Upstream channels	● IDs: 1-4 ● Type: European standard (default channel type) ● ID of the upstream channel modulation profile: 1 (by default) ● Channel central frequency (MHz): 29.8, 42.60, 49.00, and 55.4
Downstream channels	● IDs: 1-16 ● Type: European standard (default channel type) ● Channel central frequency (MHz): 602.00, 610.00, 618.00, ..., and 722.00

Procedure

- Log in to and configure the ONU.

  You can remote log in to the ONU from the OLT to perform the configuration. The user name is **root** and the password is **mduadmin**.

- Customize RF port parameters in cable mode.

  1. Configure the frequency spectrum range and channel type.

     In this example, the channel is of the European type. To change the type to North American, run the **cable** command.

  2. Configure RF port parameters for upstream channels and activate the upstream channels.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
frequency and **channel-width**	A central frequency and a frequency bandwidth determine a frequency range, within which packets are transmitted. For example, the central frequency of a European channel is 55 MHz and the frequency bandwidth is 6400 kHz. Then the frequency range of the channel is 51.8-58.2 MHz.
modulation-profile	An upstream channel modulation profile defines parameters for processing the signals transmitted over the upstream channel. You do not need to configure an upstream channel modulation profile generally. Ports automatically bind to profile 1 by default.

The following configurations are used as an example to configure RF port parameters:

- Number of upstream channels: 4
- Frequency bandwidth of the channels: 3.2 MHz (default value)

```
huawei(config)#interface cable 0/1/0
huawei(config-if-cable-0/1/0)#cable upstream 1 frequency 29.8 enable
huawei(config-if-cable-0/1/0)#cable upstream 2 frequency 42.60 enable
huawei(config-if-cable-0/1/0)#cable upstream 3 frequency 49.00 enable
huawei(config-if-cable-0/1/0)#cable upstream 4 frequency 55.40 enable
```

3. Configure RF port parameters for downstream channels and activate the downstream channels.

Parameter	Description
modulation	A greater modulation mode value for downstream channels results in a higher channel bandwidth but weaker anti-interference capability. Therefore, configure the modulation mode based on site requirements. The default modulation mode is QAM256. This example uses the default setting.

The following configuration is used as an example to configure RF parameters for downstream channels: A total of 16 downstream channels have been purchased.

```
huawei(config-if-cable-0/1/0)#cable downstream 1 frequency 602.00 enable
huawei(config-if-cable-0/1/0)#cable downstream 2 frequency 610.00 enable
huawei(config-if-cable-0/1/0)#cable downstream 3 frequency 618.00 enable
huawei(config-if-cable-0/1/0)#cable downstream 4 frequency 626.00 enable
huawei(config-if-cable-0/1/0)#cable downstream 5 frequency 634.00 enable
huawei(config-if-cable-0/1/0)#cable downstream 6 frequency 642.00 enable
huawei(config-if-cable-0/1/0)#cable downstream 7 frequency 650.00 enable
```


Copyright © Huawei Technologies Co., Ltd.

```
huawei(config-if-cable-0/1/0)#cable downstream 8 frequency 658.00 enable
huawei(config-if-cable-0/1/0)#cable downstream 9 frequency 666.00 enable
huawei(config-if-cable-0/1/0)#cable downstream 10 frequency 674.00 enable
huawei(config-if-cable-0/1/0)#cable downstream 11 frequency 682.00 enable
huawei(config-if-cable-0/1/0)#cable downstream 12 frequency 690.00 enable
huawei(config-if-cable-0/1/0)#cable downstream 13 frequency 698.00 enable
huawei(config-if-cable-0/1/0)#cable downstream 14 frequency 706.00 enable
huawei(config-if-cable-0/1/0)#cable downstream 15 frequency 714.00 enable
huawei(config-if-cable-0/1/0)#cable downstream 16 frequency 722.00 enable
```

----End

Result

1. The transmit power of the downstream channels meets site requirements.

   Run the **display cable downstream** *frameid/slotid/portid* { **all** | *channel-id* } **status** command to check whether the RF port parameters meet site requirements.

2. The signal-to-noise (SNR) ratio of the upstream channels meets site requirements.

   Run the **display cable signal quality** [*frameid/slotid/portid* [**upstream** *channel-id*]] command to check whether the RF port parameters meet site requirements. A greater SNR ratio results in better signal quality. The recommended SNR ratio is greater than 30 dB.

16.4.1.11 Configuring the HSI Service on an MA5633

A cable modem (CM) connects to a distributed cable modem termination system (D-CMTS) through a cable and provides the high-speed Internet (HSI) service for users.

Data Plan

Table 16-31 Data plan for the high-speed Internet (HSI) service

Item	Data
VLAN	ID of the HSI service VLAN (S-VLAN): 100; type of the VLAN: smart
Uplink port	0/0/1

Procedure

Step 1 Log in to and configure the ONU.

You can remote log in to the ONU from the OLT to perform the configuration. The user name is **root** and the password is **mduadmin**.

Step 2 Create an S-VLAN.

The S-VLAN is a user-side service VLAN between the optical line terminal (OLT) and the distributed cable modem termination system (D-CMTS). The OLT works in Layer 3 forwarding mode.

```
huawei(config)#vlan 100 smart
huawei(config)#port vlan 100 0/0 1
```


Copyright © Huawei Technologies Co., Ltd.

Step 3 Create a cable modem (CM) S-VLAN.

The CM S-VLAN identifies a CM service flow. After the CM S-VLAN is configured, the OLT automatically creates a CM service flow when the CM goes online.

```
huawei(config)#cable service-vlan 100
  Info: The new service VLAN will take effect after the CM is restarted, are you
 sure to modify? (y/n)[n]:y
```

----End

16.4.1.12 Configuring the DOCSIS VoD Service on an MA5633

A cable modem (CM) connects to a distributed cable modem termination system (D-CMTS) through a cable and provides the DOCSIS VoD service for users.

Context

All home services use a service VLAN (S-VLAN) and the S-VLAN is globally configured. If the S-VLAN has been configured for other home services, use the S-VLAN for the VoD service.

Data Plan

Table 16-32 Data plan for the VoD service

Item	Data
VLAN	ID of the VoD S-VLAN: 100; type of the VLAN: smart
Uplink port	0/0/1

Procedure

Step 1 Log in to and configure the ONU.

You can remote log in to the ONU from the OLT to perform the configuration. The user name is **root** and the password is **mduadmin**.

Step 2 Create an S-VLAN.

The S-VLAN is a user-side service VLAN between the optical line terminal (OLT) and the distributed cable modem termination system (D-CMTS). The OLT works in Layer 3 forwarding mode.

```
huawei(config)#vlan 100 smart
huawei(config)#port vlan 100 0/0 1
```

Step 3 Create a cable modem (CM) S-VLAN.

The CM S-VLAN identifies a CM service flow. After the CM S-VLAN is configured, the OLT automatically creates a CM service flow when the CM goes online.

Copyright © Huawei Technologies Co., Ltd.

```
huawei(config)#cable service-vlan 100
  Info: The new service VLAN will take effect after the CM is restarted, are you
 sure to modify? (y/n)[n]:y
```

----End

16.4.1.13 Configuring the EQAM VoD Service on an MA5633

If the MA5633 is equipped with a built-in EQAM module, the MA5633 sets idle downstream DOCSIS channels as EQAM channels to transmit VoD data.

Prerequisites

The MA5633 supports built-in EQAM.

Context

In multiservice operator (MSO)-oriented solutions, both HFC networks and STBs use the broadcast television QAM technology and support only RF signals.

Video data is encapsulated into IP and UDP packet headers that are transmitted on IP networks, which cannot be transmitted on HFC networks. To transmit the video data on HFC networks, the video data must be modulated into RF signals using the EQAM module.

Video data transmission on HFC networks uses existing CATV coaxial cables on the HFC networks, thereby reducing network deployment costs.

Data Plan

Table 16-33 Data plan for the VoD service

Item	Data
EQAM IP address	10.10.10.10
VLAN	ID of the VoD S-VLAN: 50; type of the VLAN: smart
Uplink port	Forwarding CM management, VoD, and multicast packets: 0/0/1
EQAM channel ID	13-16
Modulation mode	QAM 64
Symbol rate	6.875
UDP port number	501-514
Access port on the OLT	0/3/0
Uplink port on the OLT	0/5/0

Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Log in to and configure the ONU.

You can remote log in to the ONU from the OLT to perform the configuration. The user name is **root** and the password is **mduadmin**.

Step 2 Configure RF port parameters.

```
huawei(config)#interface cable 0/1/0
huawei(config-if-cable-0/1/0)#cable downstream 13 frequency 698.0 modulation qam64
enable channel-mode eqam symbol-rate 6.875
huawei(config-if-cable-0/1/0)#cable downstream 14 frequency 706.00 modulation
qam64 enable channel-mode eqam symbol-rate 6.875
huawei(config-if-cable-0/1/0)#cable downstream 15 frequency 714.00 modulation
qam64 enable channel-mode eqam symbol-rate 6.875
huawei(config-if-cable-0/1/0)#cable downstream 16 frequency 722.00 modulation
qam64 enable channel-mode eqam symbol-rate 6.875
huawei(config-if-cable-0/1/0)#quit
```

Step 3 Configure a video profile.

A video profile contains all video mappings on an EQAM module and supports batch video mapping configurations. This facilitates video mapping configuration and management.

```
huawei(config)#cable eqam video profile name vod1
huawei(config-eqam-video-profile-vod1)#mapping index 1 type spts udp-port 501
output-program 1 pmtpid 32 channel 13
huawei(config-eqam-video-profile-vod1)#mapping index 2 type spts udp-port 502
output-program 2 pmtpid 48 channel 13
huawei(config-eqam-video-profile-vod1)#mapping index 3 type spts udp-port 503
output-program 3 pmtpid 64 channel 13
huawei(config-eqam-video-profile-vod1)#mapping index 4 type spts udp-port 504
output-program 4 pmtpid 80 channel 13
huawei(config-eqam-video-profile-vod1)#mapping index 5 type spts udp-port 505
output-program 1 pmtpid 96 channel 14
huawei(config-eqam-video-profile-vod1)#mapping index 6 type spts udp-port 506
output-program 2 pmtpid 112 channel 14
huawei(config-eqam-video-profile-vod1)#mapping index 7 type spts udp-port 507
output-program 3 pmtpid 128 channel 14
huawei(config-eqam-video-profile-vod1)#mapping index 8 type spts udp-port 508
output-program 1 pmtpid 160 channel 15
huawei(config-eqam-video-profile-vod1)#mapping index 9 type spts udp-port 509
output-program 2 pmtpid 176 channel 15
huawei(config-eqam-video-profile-vod1)#mapping index 10 type spts udp-port 510
output-program 1 pmtpid 224 channel 16
huawei(config-eqam-video-profile-vod1)#mapping index 11 type spts udp-port 511
output-program 2 pmtpid 240 channel 16
huawei(config-eqam-video-profile-vod1)#mapping index 12 type spts udp-port 512
output-program 3 pmtpid 256 channel 16
huawei(config-eqam-video-profile-vod1)#mapping index 13 type spts udp-port 513
output-program 4 pmtpid 272 channel 16
huawei(config-eqam-video-profile-vod1)#mapping index 14 type spts udp-port 514
output-program 5 pmtpid 288 channel 16
huawei(config-eqam-video-profile-vod1)#quit
```


Copyright © Huawei Technologies Co., Ltd.

NOTE

To configure video mappings in batches, do as follows:

```
huawei(config)#cable eqam video profile name vod1
huawei(config-eqam-video-profile-vod1)#mapping index 1 type spTS udp-port 501
output-program 1 pmtpid 32 chan
nel 13 number 4 increment output-program 1 pmtpid 32 udp-port 1
huawei(config-eqam-video-profile-vod1)#mapping index 5 type spts udp-port 505
output-program 1 pmtpid 96 chan
nel 14 number 3 increment output-program 1 pmtpid 32 udp-port 1
huawei(config-eqam-video-profile-vod1)#mapping index 8 type spts udp-port 508
output-program 1 pmtpid 160 chan
nel 15 number 2 increment output-program 1 pmtpid 32 udp-port 1
huawei(config-eqam-video-profile-vod1)#mapping index 10 type spts udp-port 510
output-program 1 pmtpid 224 chan
nel 16 number 5 increment output-program 1 pmtpid 32 udp-port 1
```

Step 4 Configure the VoD S-VLAN.

VLAN 50 is the S-VLAN that functions between the OLT and the MA5633. The OLT works in Layer 3 forwarding mode.

```
huawei(config)#vlan 50 smart
huawei(config)#port vlan 50 0/0 1
```

Step 5 Configure a video domain.

A video domain defines the relationships between an EQAM module and an EQAM IP address, and between the S-VLAN used for video data forwarding on an EQAM module, the EQAM module, and a video profile. This facilitates data management.

```
huawei(config)#cable eqam video domain huawei
huawei(config-eqam-domain-huawei)#local ip 10.10.10.10 vlan 50
huawei(config-eqam-domain-huawei)#bind video profile name vod1 0/1/0
huawei(config-eqam-domain-huawei)#quit
```

----End

Result

The MA5633 supports packet statistics query. Based on the statistical results, you can determine whether users can order programs and whether packet loss occurs in program transmitting.

- Run the **display cable eqam video stream** command to check the TS status. If the status is **online**, the TS is functional.
- Run the **display cable eqam video statistics input** command to query packet statistics and network jitter of a TS on the video service input end.

  Check whether the program ordered by a user has been sent to the MA5633. If the program has been sent to the MA5633, check whether the program traffic is normal.
- Run the **display cable eqam video statistics output** command to query packet statistics of a TS on the video service output end.

  Check whether the TS contains the ordered program, whether the program has been sent to the STB, and whether the TS traffic is normal.

Follow-up Procedure

After configuring the MA5633, perform the following steps to configure a service channel on the OLT.

Copyright © Huawei Technologies Co., Ltd.

1. Configure an S-VLAN.

   VLAN 50 is the S-VLAN that functions between the OLT and the MA5633. The OLT works in Layer 3 forwarding mode.

   ```
   OLT(config)#vlan 50 smart
   OLT(config)#port vlan 50 0/5 0
   ```

2. Configure a service flow.

   - Configuration of a service flow:
     - Service flow ID: 3
     - S-VLAN ID: 50
     - Customer VLAN (C-VLAN) ID: 50
   - Device where upstream and downstream packet rates are limited: MA5633 (In this case, use the default traffic profile with ID 6, which does not limit the rate of a service flow. To limit packet rates, run the **traffic table ip** command to create a traffic profile and bind it to the service flow.)

   Configuration if the service is accessed using a GPON board:

   ```
   OLT(config)#service-port 3 vlan 50 gpon 0/3/0 ont 1 gemport 1 multi-service
   user-vlan 50 rx-cttr 6 tx-cttr 6
   ```

   Configuration if the service is accessed using a GE board:

   ```
   OLT(config)#service-port 3 vlan 50 eth 0/3/0 multi-service
   user-vlan 50 rx-cttr 6 tx-cttr 6
   ```

16.4.1.14 Configuring the BTV Service on an MA5633

A cable modem (CM) connects to a distributed cable modem termination system (D-CMTS) through a cable and provides the multicast service for users.

Context

All home services use a service VLAN (S-VLAN) and the S-VLAN is globally configured. If the S-VLAN has been configured for other home services, use the S-VLAN for the multicast service.

Data Plan

Table 16-34 Data plan for the multicast service

Item	Data
VLAN	ID of the multicast S-VLAN: 100; type of the VLAN: smart
Uplink ports	0/0/1

Procedure

Step 1 Log in to and configure the ONU.

Copyright © Huawei Technologies Co., Ltd.

You can remote log in to the ONU from the OLT to perform the configuration. The user name is **root** and the password is **mduadmin**.

Step 2 Create an S-VLAN.

The S-VLAN is a user-side service VLAN between the optical line terminal (OLT) and the distributed cable modem termination system (D-CMTS). The OLT works in Layer 3 forwarding mode.

```
huawei(config)#vlan 100 smart
huawei(config)#port vlan 100 0/0 1
```

Step 3 Create a cable modem (CM) S-VLAN.

The CM S-VLAN identifies a CM service flow. After the CM S-VLAN is configured, the OLT automatically creates a CM service flow when the CM goes online.

```
huawei(config)#cable service-vlan 100
  Info: The new service VLAN will take effect after the CM is restarted, are you
 sure to modify? (y/n)[n]:y
```

Step 4 Configure multicast VLAN 100.

NOTE

This configuration takes effect only after the CMs go online again.

```
huawei(config)#multicast-vlan 100
```

Step 5 Configure the Internet Group Management Protocol (IGMP) version to IGMPv3.

```
huawei(config-mvlan100)#igmp version v3
```

Step 6 Configure a multicast program generation mode.

Multicast programs can be dynamically or statically generated. For the D-CMTS, the multicast programs are dynamically generated.

```
huawei(config-mvlan100)#igmp mode off
  Are you sure to close IGMP? (y/n)[n]:y
huawei(config-mvlan100)#igmp match mode disable
```

Step 7 Configure the multicast uplink port to 0/0/1.

```
huawei(config-mvlan100)#igmp uplink-port 0/0/1
```

Step 8 Configure the IGMP mode to IGMP proxy.

```
huawei(config-mvlan100)#igmp mode proxy
  Are you sure to change IGMP mode?(y/n)[n]:y
huawei(config-mvlan100)#quit
```

Step 9 Bind CM multicast users to the multicast VLAN.

NOTE

This configuration takes effect only after the CMs go online again.

```
huawei(config)#cable multicast-vlan 100
```

Step 10 (Optional) Disable multicast DSID-based forwarding (MDF).

Multicast DSID-based forwarding is defined in data over cable service interface specification (DOCSIS) 3.0, perform this step if the CMs comply with DOCSIS 2.0.

Disable MDF if the CMTS is connected to a CM equipped with a TI chip. Otherse, the CM may go online and offline repeatedly.

Copyright © Huawei Technologies Co., Ltd.

```
huawei(config)#cable multicast mdf disable
```

Step 11 (Optional) Configure multicast user authentication.

NOTE

Perform this step if the configuration file on the CM server contains only the multicast rights profile name and the multicast rights must be configured on the D-CMTS.

The following configurations are used as an example to configure multicast user authentication:

- Multicast authentication function: enabled globally
- Maximum number of programs can be ordered if the CM does not match any rights rule: 32
- IP addresses of the multicast programs that can be ordered by multicast users: 225.1.1.1 and 225.1.1.2
- IP address of the multicast server: 192.168.20.11
- Multicast program priorities: 254 and 255

```
huawei(config)#cable multicast authorization enable max-sessions 32 default-acti
on permit
huawei(config)#cable multicast auth-profile profile-name btv1
huawei(config-multicast-profile-btv1)#rule 1 priority 255 group-ip 225.1.1.1 gro
up-ip-mask 24 src-ip 192.168.20.11 src-ip-mask 24 permit
huawei(config-multicast-profile-btv1)#rule 1 priority 254 group-ip 225.1.1.2 gro
up-ip-mask 24 src-ip 192.168.20.11 src-ip-mask 24 permit
```

Step 12 (Optional) Configure cable multicast version.

```
huawei(config)#cable multicast igmp-version v3
```

----End

16.4.1.15 Configuring the Dynamic PacketCable Service on an MA5633

A cable modem (CM) connects to a distributed cable modem termination system (D-CMTS) through a cable and provides the dynamic PacketCable service for users.

Context

Table 16-35 Data plan for the PacketCable service

Item	Data
Uplink port	0/0/1
VLAN	ID of the PacketCable service VLAN (S-VLAN): 100; type of the VLAN: smart ID of the common open policy service (COPS) connection VLAN: 1000
IP address for creating a COPS connection to an IP multimedia subsystem (IMS) or a softswitch	192.168.60.3/24 (in the same network segment as the IMS or softswitch or can communicate with the IMS or softswitch)

Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Log in to and configure the ONU.

You can remote log in to the ONU from the OLT to perform the configuration. The user name is **root** and the password is **mduadmin**.

Step 2 Create a service VLAN (S-VLAN).

NOTE

All home services use an S-VLAN and the S-VLAN is globally configured. If the S-VLAN has been configured for other home services, use the S-VLAN in steps **Step 1** and **Step 2**.

The S-VLAN is a user-side service VLAN between the optical line terminal (OLT) and the D-CMTS. The OLT works in Layer 3 forwarding mode.

```
huawei(config)#vlan 100 smart
huawei(config)#port vlan 100 0/0 1
```

Step 3 Create a cable modem (CM) S-VLAN.

The CM S-VLAN identifies a CM service flow. After the CM S-VLAN is configured, the OLT automatically creates a CM service flow when the CM goes online.

```
huawei(config)#cable service-vlan 100
  Info: The new service VLAN will take effect after the CM is restarted, are you
 sure to modify? (y/n)[n]:y
```

Step 4 Configure the Layer 3 interface for COPS connections.

```
huawei(config)#vlan 1000 smart
huawei(config)#interface vlanif 1000
huawei(config-if-vlanif1000)#ip address 192.168.60.3 24
huawei(config-if-vlanif1000)#quit
huawei(config)#port vlan 1000 0/0 1
```

Step 5 Configure a COPS connection.

The following configurations are used as an example to configure a COPS connection:

- COPS policy enforcement point (PEP) ID: IP address of the Layer 3 interface for the COPS connection
- Transmit and receive buffer for TCP sockets: 12 KB
- Differentiated services code point (DSCP) priority of COPS packets: ef

```
huawei(config)#cops pepid 192.168.60.3
huawei(config)#cops tcp window 12
huawei(config)#cops ip dscp ef
```

Step 6 Configure PacketCable parameters.

PacketCable 1.x parameter settings are as follows:

- Embedded media terminal adapter (EMTA) creating a dynamic media stream: permitted
- Other parameters: default settings

```
huawei(config)#packetcable 1dotx enable
huawei(config)#packetcable authorize common-docsis-mta enable
huawei(config)#packetcable multimedia enable
```

----End

Copyright © Huawei Technologies Co., Ltd.

16.4.1.16 Verifying Services

To facilitate service verification, an MA5633 supports multiple remote service verification methods, such as Dynamic Host Configuration Protocol (DHCP) dialup emulation tests. This allows commissioning and configuration engineers to remotely verify services. In addition, this section describes how to verify services on site.

Prerequisites

- The MA5633 is properly connected to the upper-layer network.
- The DHCP server, Trivial File Transfer Protocol (TFTP) server, and softswitch or IP multimedia subsystem (IMS) have been configured.

Procedure

- Log in to and configure the ONU.

  You can remote log in to the ONU from the OLT to perform the configuration. The user name is **root** and the password is **mduadmin**.

- Perform a DHCP dialup emulation test.

  In this test, a cable modem (CM) is emulated on the MA5633 to apply to the DHCP server for an IP address. This checks whether the MA5633 can communicate with the DHCP server and verifies CM DHCP configurations on the DHCP relay, proxy, and server.

  1. Run the **simulate dhcp start cm** *mac-address* [**option60** *option60*] command to start a DHCP dialup emulation test.

     NOTE

     You can run the **simulate dhcp stop** command to stop the DHCP emulation.

  2. Run the **display simulation dhcp** command to query the results of the DHCP dialup emulation test.
  3. Check whether the **User IP** has obtained an IP address.

- Check the CM status.

  Run the **display cable modem** command to query the CM status in **Status**.

```
huawei(config)#display cable modem  all

------------------------------------------------------------------------------
-
 Idx   MAC            IP              I/F          Status   Prim  Num Ver  DS
RX
                                                           SID   CPE
Power

------------------------------------------------------------------------------
-
 1     0023-ED6F-21A3 192.168.1.118   0/1/0/U4     ol-pt    1     0   D2.0
-

------------------------------------------------------------------------------
-
 Total:
1
 ol: 0, ol-ptd: 0, ol-pt: 1, ol-d: 0, wol: 0, wol-ptd: 0, wol-pt: 0, wol-d:
0,
pol: 0, pol-ptd: 0, pol-pt: 0, pol-d: 0, offline: 0, rej-m: 0, rej-pt: 0, rej-
```


Copyright © Huawei Technologies Co., Ltd.

```
o:
 0, init: 0, init-rc: 0, DHCP: 0, DHCP-O: 0, DHCP-R: 0, DHCP-C: 0, REG:
0
 Note: 1. Idx is the index of a
CM.
       2. The downstream received power is in the unit of
dBmV.
       3. In status, "ol" means online, "rej" means reject.
```

The following table lists the CM status and handling suggestions.

CM Status	Description	Handling Suggestion
init	Indicates that the CM initialization ranging message is received.the CM initialization.	If a CM is always in the ranging state, the ranging fails. Then check radio frequency (RF) line indicators and detect line faults.
init-rc	Indicates that the CM initialization ranging is complete.	No action is required. The ranging of the CM is complete.
DHCP	Indicates that the DHCP discovery from the CM is received.	If a CM initiates a DHCP request but does not obtain an IP address, check the DHCP server, routing between the OLT and the DHCP server, and DHCP server parameter settings.
● DHCP-O ● DHCP-R ● DHCP-C	● DHCP-O: indicates that the offer from the DHCP server is received. ● DHCP-R: indicates that the DHCP request from the CM is received. ● DHCP-C: indicates that the acknowledge from the DHCP server is received.	The DHCP server has assigned an IP address to the CM and sent configuration file name and IP address of the TFTP or ToD server to the CM using the Option 67 and Option 66 fields (the Option 67 field carries the configuration file name and the Option 66 field carries the IP address of the TFTP or ToD server). If the CM is always in the DHCP-C state, the CM fails to obtain the configuration file. Then check the TFTP server, routing between the OLT and the TFTP server, and TFTP server parameter settings.
REG	Indicates that a registration is started.	If the CM is always in the register state, the CM obtains an incorrect configuration file. Then change the configuration file.

Copyright © Huawei Technologies Co., Ltd.

CM Status	Description	Handling Suggestion
● ol ● ol-pt ● ol-ptd ● ol-d ● wol ● wol-pt ● wol-ptd ● wol-d ● pol ● pol-pt ● pol-ptd	● ol: indicates that the CM is online. (valid only for CMs complying with DOCSIS 2.0) ● ol-pt: indicates that the CM is online and passes the BPI authentication. (valid only for CMs complying with DOCSIS 2.0) ● ol-ptd: indicates that the CM is online and passes the BPI authentication, and NetAccessEnable is disabled. (valid only for CMs complying with DOCSIS 2.0) ● ol-d: indicates that the CM is online and NetAccessEnable is disabled. (valid only for CMs complying with DOCSIS 2.0) ● wol: indicates that the CM is online and all channels bound to the CM are available. (valid only for CMs complying with DOCSIS 3.0) ● wol-pt: indicates that the CM is online and passes the BPI authentication, and all channels bound to the CM are available. (valid only for CMs complying with DOCSIS 3.0) ● wol-ptd: indicates that the CM is online and passes the BPI authentication, NetAccessEnable is disabled, and all channels bound to the CM are available. (valid only for CMs complying with DOCSIS 3.0) ● wol-d: indicates that the CM is online, NetAccessEnable is disabled, and all channels bound to the CM are available. (valid only for CMs complying with DOCSIS 3.0) ● pol: indicates that the CM is online and some channels	No action is required. The status indicates that the CM has registered

Copyright © Huawei Technologies Co., Ltd.

CM Status	Description	Handling Suggestion
● pol-d	bound to the CM are available. (valid only for CMs complying with DOCSIS 3.0) ● pol-pt: indicates that the CM is online and passes the BPI authentication, and some channels bound to the CM are available. (valid only for CMs complying with DOCSIS 3.0) ● pol-ptd: indicates that the CM is online and passes the BPI authentication, NetAccessEnable is disabled, and some channels bound to the CM are available. (valid only for CMs complying with DOCSIS 3.0) ● pol-d: indicates that the CM is online, NetAccessEnable is disabled, and some channels bound to the CM are available. (valid only for CMs complying with DOCSIS 3.0)	with the OLT and can correctly transmit and receive services.
offline	Indicates the offline status.	If the CM is in the offline state, check the power status, noise, and channel frequency of the CM.
● rej-m ● rej-pt ● rej-o	● rej-m: indicates that the MIC verification fails. ● rej-pt: indicates that the BPI authentication fails. ● rej-o: indicates that the authentication reject due to other reasons.	If the CM is in the reject state, no service flow can be created. Then check the CM authentication and CM message integrity check (MIC), and check whether class of service (COS) parameters specified in the CM configuration file are supported by the OLT.

- Verify that home services can be provisioned.
  1. After the CM is installed at a user home and commissioned, the user can watch TV programs.
  2. After the high-speed Internet (HSI) service is provisioned, the user can access the Internet from a PC.
  3. After the VoD service is provisioned, the user can order programs.
  4. After the VoIP service is provisioned, the user can make and receive phone calls.

Copyright © Huawei Technologies Co., Ltd.

5. After the multicast service is provisioned, the user can watch ordered multicast programs.

----End

16.4.2 L2VPN Enterprise Service Networking

In L2VPN enterprise service networking, an MA5633 connects to cable modems (CMs) through radio frequency (RF) ports, and the CMs connect to switches to provide the L2VPN service for users. This section describes how to configure the optical line terminal (OLT) and the MA5633 to provision the L2VPN service.

NOTE

Configuration procedures are the same for IPv6 and IPv4 networks except in "onfigure Dynamic Host Configuration Protocol (DHCP) rela" and "onfigure a route".

16.4.2.1 Service Requirements and Usage Scenario

Service Requirements

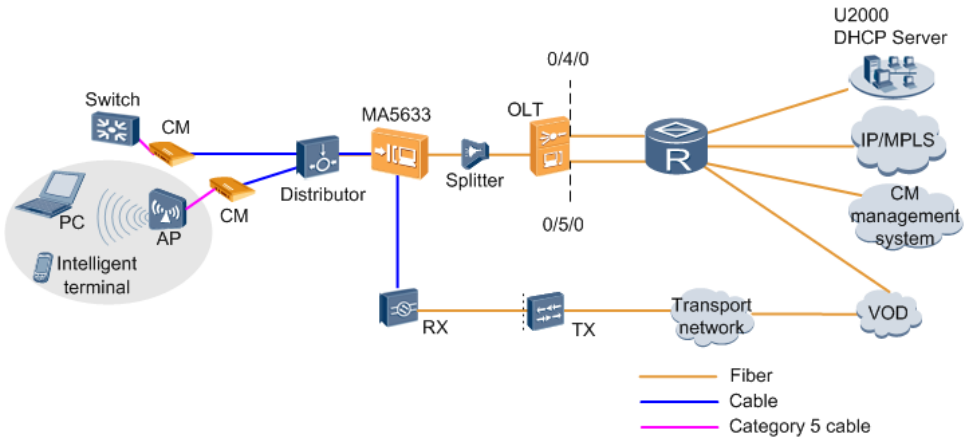
An enterprise requires the provisioning of the L2VPN service.

Usage Scenario

As shown in **Figure 16-11**, an MA5633 is deployed on an optical node and cable modems (CMs) are deployed at enterprises. The CMs connect to radio frequency (RF) ports on the MA5633 through cables.

- A CM provides the enterprise service through a switch, which connects to enterprise users.
- Enterprise users access the Internet through Dynamic Host Configuration Protocol (DHCP) dialup.

Figure 16-11 L2VPN enterprise service networking

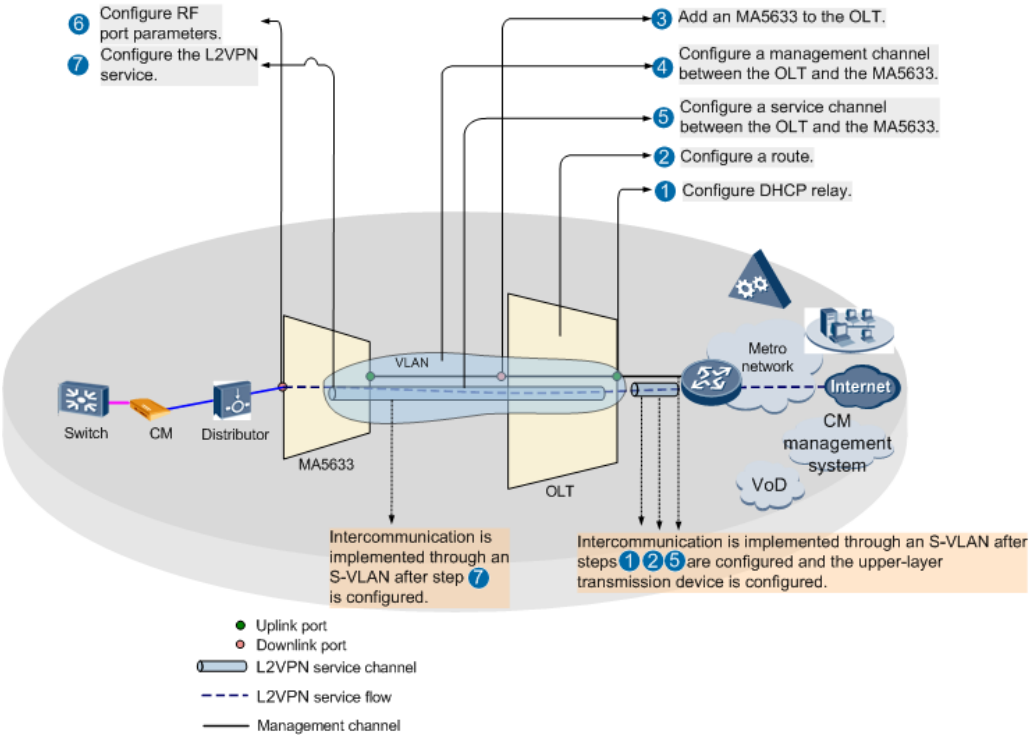


16.4.2.2 Configuration Process

Copyright © Huawei Technologies Co., Ltd.

Figure 16-12 shows the configuration roadmap for the L2VPN service networking.

Figure 16-12 Configuration roadmap for the L2VPN service networking



NOTE

Before logging in to the MA5633 to configure services on it, ensure that the MA5633 has been properly connected.

The following table describes the configuration steps.

Configuration Object	Step	Description
OLT	● IPv4: **Configure Dynamic Host Configuration Protocol (DHCP) relay.** ● IPv6: **Configure Dynamic Host Configuration Protocol (DHCP) relay (IPv6).**	This section describes how to configure Dynamic Host Configuration Protocol (DHCP) relay so that cable modems (CMs) can obtain IP addresses in different network segments.
	● IPv4: **Configure a route.** ● IPv6: **Configure a route (IPv6).**	This section describes how to implement network communication by configuring a route in Layer 3 networking with an optical line terminal (OLT). Through the route, packets are forwarded at Layer 3 between the OLT and its upper-layer devices or servers.

Copyright © Huawei Technologies Co., Ltd.

Configuration Object	Step	Description
	Add a D-CMTS to the OLT.	You can configure a distributed cable modem termination system (D-CMTS) only after adding it to an optical line terminal (OLT).
	Configure a management channel between the OLT and the D-CMTS.	This section describes how to configure a management channel between an optical line terminal (OLT) and a distributed cable modem termination system (D-CMTS). After the configuration, you can log in to the D-CMTS from the OLT and configure the D-CMTS.
	Configure a service channel between the OLT and the D-CMTS.	This section describes how to configure a service channel between an optical line terminal (OLT) and a distributed cable modem termination system (D-CMTS). After the configuration, the service channel forwards service packets on the D-CMTS based on the planned VLAN and forwarding policy.
MA5633	**Configure radio frequency (RF) port parameters.**	Radio frequency (RF) port parameters define the frequency spectrum range for signal transmission and modulation mode. The configuration of RF port parameters implements data service transmission over cables.
	Configure the L2VPN service.	None
	Verify the configured service.	A D-CMTS supports multiple remote service verification methods. This allows commissioning and configuration engineers to remotely verify services. 1. A DHCP dialup emulation test checks whether the D-CMTS can communicate with the DHCP server and verifies CM DHCP configurations on the DHCP relay, proxy, and server. 2. The status of a CM can be queried. Based on the information, you can determine whether the CM is online.

Copyright © Huawei Technologies Co., Ltd.

16.4.2.3 Configuring DHCP Relay

This section describes how to configure Dynamic Host Configuration Protocol (DHCP) relay so that cable modems (CMs) can obtain IP addresses in different network segments.

Prerequisites

The upper-layer router, DHCP server, and Trivial File Transfer Protocol (TFTP) server of an optical line terminal (OLT) have been configured.

Data Plan

Table 16-36 DHCP data plan for the OLT

Item	Data
VLAN	ID of the CM management S-VLAN: 200; type of the VLAN: smart
DHCP server group parameters	IP address of the DHCP domain gateway for CMs: 10.10.224.1; domain name: docsis

Table 16-37 Data plan for the upper-layer devices of the OLT

Item	IP Address
Layer 3 interfaces connecting the router to the OLT	● Forwarding DHCP and broadband packets: 11.11.11.11 ● Forwarding CM management packets: 11.11.12.11
IP address of the DHCP server	DHCP server assigning IP addresses to CMs and media terminal adapters (MTAs): 192.168.10.10-192.168.10.11

Procedure

Step 1 Set the IP address of the VLAN Layer 3 interface.

```
huawei(config)#vlan 100 smart
huawei(config)#interface vlanif 100
huawei(config-if-vlanif100)#ip address 10.10.224.1 255.255.255.0     //Set the IP
address of the DHCP domain gateway for CMs.
huawei(config-if-vlanif100)#quit
```

Step 2 Configure the working mode of the DHCP relay to Layer 3 Option 60.

In DHCP Option 60 mode, a DHCP server group is selected according to the Option 60 domain name in DHCP packets. Users in this mode are identified by domain information of packets, which differentiates various service types in a VLAN. Ensure that the Option 60 domain name and the DHCP server group bound to the Option 60 domain name are configured beforehand.

Copyright © Huawei Technologies Co., Ltd.

```
huawei(config)#dhcp mode layer-3 Option60
  Several minutes may be required and no action can be taken during this period
  Are you sure to perform this operation? (y/n)[n]: y
```

Step 3 Set the IP addresses of the servers in a DHCP server group.

```
huawei(config)#dhcp-server 0 ip 192.168.10.10 192.168.10.11    //Configure DHCP
server group 0 to assign IP addresses to CMs.
```

Step 4 Create a DHCP Option 60 domain.

```
huawei(config)#dhcp domain docsis   //Create Option 60 domain name docsis for CMs.
huawei(config-dhcp-domain-docsis)#dhcp-server 0 vlan 100       //Bind DHCP server
group 0 to the DHCP domain where the CMs locate. After the configuration, the CMs
in the DHCP domain are corresponded to DHCP server group 0.
huawei(config-dhcp-domain-docsis)#quit
```

Step 5 Set the IP address of the gateway for the DHCP domain.

```
huawei(config)#interface vlanif 100
huawei(config-if-vlanif100)#dhcp domain docsis gateway 10.10.224.1    //Set the IP
address of the gateway for the CM domain to 10.10.224.1.
huawei(config-if-vlanif100)#quit
```

----End

16.4.2.4 Configuring a Route

This section describes how to implement network communication by configuring a route in Layer 3 networking with an optical line terminal (OLT). Through the route, packets are forwarded at Layer 3 between the OLT and its upper-layer devices or servers.

Prerequisites

The upper-layer router of an OLT has been configured.

Data Plan

Table 16-38 Data plan for the Layer 3 interfaces on the network side

Item	IP Address
Layer 3 interfaces on the OLT network side	Forwarding Dynamic Host Configuration Protocol (DHCP) packets: ● VLAN ID: 2004 ● Port number: 0/4/0 ● IP address: 11.11.11.10/24 Forwarding cable modem (CM) management packets: ● VLAN ID: 2005 ● Port number: 0/5/0 ● IP address: 11.11.12.10/24
Layer 3 interfaces connecting the router to the OLT	● Forwarding DHCP packets: 11.11.11.11 ● Forwarding CM management packets: 11.11.12.11

Copyright © Huawei Technologies Co., Ltd.

Item	IP Address
Upper-layer servers of the OLT	● DHCP server assigning IP addresses to CMs and media terminal adapters (MTAs): 192.168.10.10-192.168.10.11 ● CM management system: 192.168.20.1

Procedure

Step 1 Create Layer 3 VLAN interfaces on the network side.

1. Create VLANs and configure their uplink ports.
   - VLAN 2004 is of the smart VLAN type and used for forwarding DHCP packets. Add uplink port 0/4/0 to VLAN 2004.
   - VLAN 2005 is of the smart VLAN type and used for forwarding CM management packets. Add uplink port 0/5/0 to VLAN 2005.

```
huawei(config)#vlan 2004 to 2006 smart
huawei(config)#port vlan 2004 0/4 0
huawei(config)#port vlan 2005 0/5 0
```

2. (Optional) Create native VLANs for Ethernet outbound ports.

   Packets between the OLT and its upper-layer router are forwarded at Layer 3 and no VLAN information is required. The created native VLANs remove VLAN tags from the packets transmitted out of Ethernet ports.

```
huawei(config)#interface eth 0/4
huawei(config-if-eth-0/4)#native-vlan 0 vlan 2004    //Remove VLAN tags from
the packets transmitted out of the 0/4/0 port.
huawei(config-if-eth-0/4)#quit
huawei(config)#interface eth 0/5
huawei(config-if-eth-0/5)#native-vlan 0 vlan 2005    //Remove VLAN tags from
the packets transmitted out of the 0/5/0 port.
huawei(config-if-eth-0/5)#quit
```

3. Create Layer 3 VLAN interfaces.
   a. Create a Layer 3 interface for VLAN 2004, through which DHCP packets are forwarded.

```
huawei(config)#interface vlanif 2004
huawei(config-if-vlanif2004)#ip address 11.11.11.10 255.255.255.0
huawei(config-if-vlanif2004)#quit
```

   b. Create a Layer 3 interface for VLAN 2005, through which CM management packets are forwarded.

```
huawei(config)#interface vlanif 2005
huawei(config-if-vlanif2005)#ip address 11.11.12.10 255.255.255.0
huawei(config-if-vlanif2005)#quit
```

Step 2 Configure static routes to implement the communication between the OLT and its upper-layer devices.

```
huawei(config)#ip route-static 192.168.20.0 255.255.255.0 11.11.12.11     //CM
management and VoD packets are forwarded through the Layer 3 interface of VLAN
2005.
huawei(config)#ip route-static 192.168.10.0 255.255.255.0 11.11.11.11     //DHCP
packets are forwarded through the Layer 3 interface of VLAN 2004.
```


Copyright © Huawei Technologies Co., Ltd.

NOTE

The interconnected router must set static routes and add the routes to dynamic routes.

----End

Result

The OLT can communicate with its upper-layer devices. To check network connectivity between two devices, run the **ping** and **tracert** commands.

The configured static routes can be queried in an IPv4 routing table by running the **display ip routing-table** command.

16.4.2.5 Configuring DHCP Relay (IPv6)

This section describes how to configure DHCPv6 relay so that CMs can obtain IP addresses in different network segments.

Prerequisites

The upper-layer router, DHCP server, and Trivial File Transfer Protocol (TFTP) server of an OLT have been configured.

Data Plan

Table 16-39 data plan

Configuration Item	Data
Terminal-side of CM	network segment of CM: 2001:0db8:0001::/64
User-side of OLT	IP address of the gateway for the DHCP domain of CMs: 2001:0db8:0001::1/64; domain name: **docsis**
Network-side of OLT	Forwarding DHCP and broadband packets: ● VLAN ID: 2004 ● Port number: 0/4/0 ● IP address: 2001:0db8:0007::12/64 Forwarding CM management packets, multicast packets, and VoD packets: ● VLAN ID: 2005 ● Port number: 0/5/0 ● IP address: 2001:0db8:0008::13/64
Router	● IP address of the Layer 3 interface for forwarding DHCP and broadband packets: 2001:0db8:0007::6/64 ● IP address of the Layer 3 interface for forwarding CM management packets: 2001:0db8:0008::7/64

Copyright © Huawei Technologies Co., Ltd.

Configuration Item	Data
Server	● IP addresses of DHCP servers: – DHCP server allocating IP addresses for CMs: 2001:0db8:0006::8/64-2001:0db8:0006::9/64 – DHCP server allocating IP addresses for PCs: 2001:0db8:0006::10/64-2001:0db8:0006::11/64 ● IP addresses of the CM management system: 2001:0db8:0011::14/64-2001:0db8:0011::16/64

Procedure

Step 1 Configure a CM service provisioning mode, which can be IPv6 (preferentially used), APM, or DPM (used for dual-stack service provisioning). Select a mode based on site requirements.

```
huawei(config)#interface cable 1/1/0
huawei(config-if-cable-1/1/0)#cable ip-mode dpm
huawei(config-if-cable-1/1/0)#quit
```

Step 2 Configure the IP address of the VLAN Layer 3 interface.

```
huawei(config)#ipv6      //Enable IPv6 packet forwarding.
huawei(config)#vlan 100
huawei(config)#interface vlanif 100
huawei(config-if-vlanif100)#ipv6 enable     //Enable IPv6 on ports.
huawei(config-if-vlanif100)#undo ipv6 nd ra halt       //enables a router to send
RA messages.
huawei(config-if-vlanif100)#ipv6 nd autoconfig managed-address-flag     //Configure
the state-based auto-configuration address flag bit. The host obtains an IPv6
address using the state-based automatic configuration.
huawei(config-if-vlanif100)#ipv6 address 2001:0db8:0001::1/64     //Configure the
IP address of the gateway for the DHCP domain of CMs.
huawei(config-if-vlanif100)#quit
```

Step 3 Enable duplicate address detect (DAD) proxy, which prevents repeated link local addresses (LLAs) on the user side.

After receiving a DAD packet sent from the user side with destination IP address LLA, the OLT with DAD proxy enabled checks user online information based on the destination IP address and VLAN. If a user with the same IP address in the VLAN has been online, the OLT makes a response and prohibits the new user from going online. Otherwise, the OLT does not make a response.

```
huawei(config)#ipv6 dad proxy enable
huawei(config)#vlan service-profile profile-id 10
huawei(config)#vlan bind service-profile 100 profile-id 10
huawei(config-vlan-srvprof-10)#ipv6 dad proxy enable     //DAD proxy takes effect
after it is enabled at system level and VLAN service profile level.
```

Step 4 Configure the working mode of DHCP relay to Layer 3 Option 16.

Option 16 is an option with code 16 in DHCPv6 packets, which identifies terminal types. In DHCPv6 Option 16 mode, packets select a DHCPv6 server based on the Option 16 domain. Therefore, in DHCPv6 Option 16 mode, packets select a DHCPv6 server based on terminal types.

```
huawei(config)#dhcpv6 mode layer-3 option16
  Several minutes may be required and no action can be taken during this period
  Are you sure to perform this operation? (y/n)[n]: y
```


Copyright © Huawei Technologies Co., Ltd.

Step 5 Configure the IP addresses of the servers in a DHCP server group.

```
huawei(config)#dhcpv6-server 0 ipv6 2001:0db8:0006::8/64 2001:0db8:0006::9/64    //
Configure DHCP server group 0 to allocate IP addresses for CMs.
```

Step 6 Create DHCP Option 16 domains.

```
huawei(config)#dhcp domain docsis   //Create Option 16 domain docsis for CMs.
huawei(config-dhcp-domain-docsis)#dhcpv6-server 0 vlan 100      //Bind DHCP server
group 0 to the DHCP domain of CMs. After the configuration, the CMs in this DHCP
domain are mapped to DHCP server group 0.
huawei(config-dhcp-domain-docsis)#quit
```

Step 7 Configure the IP addresses of the gateways for DHCP domains.

```
huawei(config)#interface vlanif 100
huawei(config-if-vlanif100)#dhcpv6 domain docsis gateway 2001:0db8:0001::1/64    //
Configure the IP address of the gateway for the DHCP domain of CMs.
huawei(config-if-vlanif100)#quit
```

----End

16.4.2.6 Configuring a Route (IPv6)

This section describes how to implement network communication by configuring a route in Layer 3 networking with an OLT. Through the route, the OLT can forward packets at Layer 3 between the OLT and its upper-layer devices or servers.

Prerequisites

The upper-layer router of the OLT has been configured.

Data Plan

Table 16-40 data plan

Configuration Item	Data
Terminal-side of CM	network segment of CM: 2001:0db8:0001::/64
User-side of OLT	IP address of the gateway for the DHCP domain of CMs: 2001:0db8:0001::1/64; domain name: **docsis**
Network-side of OLT	Forwarding DHCP and broadband packets: ● VLAN ID: 2004 ● Port number: 0/4/0 ● IP address: 2001:0db8:0007::12/64 Forwarding CM management packets, multicast packets, and VoD packets: ● VLAN ID: 2005 ● Port number: 0/5/0 ● IP address: 2001:0db8:0008::13/64

Copyright © Huawei Technologies Co., Ltd.

Configuration Item	Data
Router	● IP address of the Layer 3 interface for forwarding DHCP and broadband packets: 2001:0db8:0007::6/64 ● IP address of the Layer 3 interface for forwarding CM management packets: 2001:0db8:0008::7/64
Server	● IP addresses of DHCP servers: – DHCP server allocating IP addresses for CMs: 2001:0db8:0006::8/64-2001:0db8:0006::9/64 – DHCP server allocating IP addresses for PCs: 2001:0db8:0006::10/64-2001:0db8:0006::11/64 ● IP addresses of the CM management system: 2001:0db8:0011::14/64-2001:0db8:0011::16/64

Procedure

Step 1 Create VLAN Layer 3 interfaces on the network side.

1. Create VLANs and add an uplink port to them, respectively.
   - VLAN 2004 used for forwarding DHCP packets is a smart VLAN. Add uplink port 0/4/0 to VLAN 2004.
   - VLAN 2005 used for forwarding CM management packets is a smart VLAN. Add uplink port 0/5/0 to VLAN 2005.

```
huawei(config)#vlan 2004 to 2005 smart
huawei(config)#port vlan 2004 0/4 0
huawei(config)#port vlan 2005 0/5 0
```

2. (Optional) Create native VLANs for Ethernet outbound ports.

   Packets between the OLT and its upper-layer router are forwarded at Layer 3 and no VLAN tag is required. The created native VLANs remove VLAN tags from the packets transmitted out of Ethernet ports.

```
huawei(config)#interface eth 0/4
huawei(config-if-eth-0/4)#native-vlan 0 vlan 2004    //The packets transmitted
out of port 0/4/0 are untagged.
huawei(config-if-eth-0/4)#quit
huawei(config)#interface eth 0/5
huawei(config-if-eth-0/5)#native-vlan 0 vlan 2005    //The packets transmitted
out of port 0/5/0 are untagged.
huawei(config-if-eth-0/5)#quit
```

3. Create VLAN Layer 3 interfaces.
   a. Create the Layer 3 interface of VLAN 2004, through which DHCP packets are forwarded.

```
huawei(config)#interface vlanif 2004
huawei(config-if-vlanif2004)#ipv6 address 2001:0db8:0007::12/64
huawei(config-if-vlanif2004)#quit
```

   b. Create the Layer 3 interface of VLAN 2005, through which CM management packets are forwarded.

Copyright © Huawei Technologies Co., Ltd.

```
huawei(config)#interface vlanif 2005
huawei(config-if-vlanif2005)#ipv6 address 2001:0db8:0008::13/64
huawei(config-if-vlanif2005)#quit
```

Step 2 Configure static routes for the communication between the OLT and its upper-layer devices.

```
huawei(config)#ipv6 route-static 2001:0db8:0006::/64 2001:0db8:0008::7/64     //CM
management packets are forwarded through the Layer 3 interface of VLAN 2005.
huawei(config)#ipv6 route-static 2001:0db8:0011::/64 2001:0db8:0007::6/64     //
DHCP packets are forwarded through the Layer 3 interface of VLAN 2004.
```

NOTE

Configure static routes on the router connected to the OLT. In addition, add the static routes to dynamic ones.

----End

Result

The OLT can communicate with its upper-layer devices. To check network connectivity between two devices, run the **ping ipv6** and **tracert ipv6** commands.

The configured static routes can be queried in an IPv6 routing table by running the **display ipv6 routing-table** command.

16.4.2.7 Adding a D-CMTS to an OLT

You can configure a distributed cable modem termination system (D-CMTS) only after adding it to an optical line terminal (OLT).

Prerequisites

The MA5633 management policy is set to **stand-alone**. To do so, run the **sysman centralized-mgmt primary** command.

Context

- When adding a D-CMTS to an OLT, bind the following profiles to the D-CMTS: dynamic bandwidth allocation (DBA) profile, line profile, and alarm profile. For details about the functions and configuration method of each profile, see **Table 16-41**.

Table 16-41 D-CMTS profiles

Profile	Function	Command
DBA profile	Describes GPON traffic parameters. A transmission container (T-CONT) is bound to a DBA profile for dynamic bandwidth allocation. This improves the upstream bandwidth usage.	Command for querying a DBA profile: **display dba-profile** Command for adding a DBA profile: **dba-profile add**

Copyright © Huawei Technologies Co., Ltd.

Profile	Function	Command
Line profile	Describes the binding between a T-CONT and a DBA profile, quality of service (QoS) mode of a service flow, and mapping from a GEM port to D-CMTS services.	Command for querying a line profile: **display ont-lineprofile** Command for adding a line profile: **ont-lineprofile**
Alarm profile	Contains a series of alarm thresholds for measuring and monitoring the performance of activated D-CMTS lines.	Command for querying an alarm profile: **display gpon alarm-profile** Command for adding an alarm profile: **gpon alarm-profile add**

- Add a D-CMTS using either of the methods listed in the following table based on site requirements.

Method	Usage Scenario	Command
Add a D-CMTS in offline mode.	You have obtained the password or serial number (SN) of the D-CMTS.	Run the **ont add** command to add the D-CMTS to an OLT.
Add an online D-CMTS and confirm the automatically discovered D-CMTS.	You do not know the password or SN of the D-CMTS.	In GPON mode, run the **port ont-auto-find** command to enable the D-CMTS automatic discovery function on GPON ports. Then run the **ont confirm** command to add the D-CMTS.

Data Plan

Table 16-42 Key data plan

Item	Data
DBA profile	Profile name: PrivateLine Type: type4 Maximum bandwidth: 1000 Mbit/s

Copyright © Huawei Technologies Co., Ltd.

Item	Data
Line profile	Profile ID: 10, bound to DBA profile **PrivateLine** GPON encapsulation mode (GEM) port IDs: 0 and 1 T-CONT ID: 5
Networking data	Port: 0/3/1 D-CMTS ID: 1 D-CMTS authentication mode: SN D-CMTS SN: 48575443E6D8B541 Management VLAN: 8 Service VLAN: 200

Procedure

Step 1 Configure D-CMTS profiles.

D-CMTS profiles include a DBA profile, a line profile, and an alarm profile.

1. Configure a DBA profile.

   Run the **display dba-profile** command to query DBA profiles existing in the system. If the existingDBA profiles do not meet service requirements, run the **dba-profile add** command to add a DBA profile.

   ```
   huawei(config)#dba-profile add profile-name PrivateLine type4 max 1000000
   ```

2. Configure a line profile.

   Add line profile 10 and bind T-CONT 5 to DBA profile **PrivateLine**. In this way, the T-CONT provides flexible DBA solutions based on the configurations in the DBA profile.

   ```
   huawei(config)#ont-lineprofile gpon profile-id 10
   huawei(config-gpon-lineprofile-10)#tcont 5 dba-profile-name PrivateLine
   ```

   The following configurations are used as an example to add a line profile:

   - Index of the GEM port for carrying management service flows: 0
   - Index of the GEM port for carrying L2VPN service flows: 1
   - ID of the T-CONT that GEM ports 0 and 1 are bound: 5
   - QoS mode: priority-queue (default)
   - Queue priority of GEM ports 0 and 1: 3, 1

   NOTE

   When the QoS mode is PQ, the default queue priority is 0.

   huawei(config-gpon-lineprofile-10)#**gem add 0 eth tcont 5 priority-queue 3**

   huawei(config-gpon-lineprofile-10)#**gem add 1 eth tcont 5 priority-queue 1**

- Mode of the mapping from the GEM port to D-CMTS services: VLAN (default)
- Index of the GEM port to which the management service flows in VLAN 8 are mapped: 0
- Index of the GEM port to which the service flows in VLAN 200 are mapped: 1

Copyright © Huawei Technologies Co., Ltd.

```
huawei(config-gpon-lineprofile-10)#mapping-mode vlan
huawei(config-gpon-lineprofile-10)#gem mapping 0 0 vlan 8
huawei(config-gpon-lineprofile-10)#gem mapping 1 1 vlan 200
```

Run the **commit** command to make the configured parameters take effect.

```
huawei(config-gpon-lineprofile-10)#commit
huawei(config-gpon-lineprofile-10)#quit
```

(Optional) Configure an alarm profile.

- The ID of the default GPON alarm profile is 1. In this profile, the thresholds for all alarm parameters in the default alarm profile are 0, which indicates that no alarm is generated.
- This section uses the default alarm profile and therefore the alarm profile does not need to be configured.
- To add an alarm profile for monitoring the performance of activated D-CMTS lines, run the **gpon alarm-profile add** command.

Step 2 Add a D-CMTS to an OLT.

The D-CMTS connects to a GPON port on the OLT through an optical fiber. You can configure the D-CMTS only after adding it to the OLT.

1. Add a D-CMTS.

   The following configurations are used as an example to add a D-CMTS: The management mode is SNMP; the ID of the line profile bound to the D-CMTS is 10.

   To add a D-CTMS in offline mode, do as follows:

```
huawei(config)#interface gpon 0/3
huawei(config-if-gpon-0/3)#ont add 1 1 sn-auth 48575443E6D8B541 snmp ont-
lineprofile-id
 10 desc MA5633_0/3/1/1_lineprofile10
```

   To automatically find a D-CMTS, do as follows:

```
huawei(config)#interface gpon 0/3
huawei(config-if-gpon-0/3)#port 1 ont-auto-find enable
huawei(config-if-gpon-0/3)#display ont autofind 1
   //This command displays the information about all automatically discovered
D-CMTSs that are connected to the GPON port through an optical splitter.

   ------------------------------------------------------------
   Number              : 1
   F/S/P               : 0/3/1
   Ont SN              : 48575443E6D8B541
   Password            : 0x3030303030303030(0000000000)
   Loid                : 00000000000000000000000000
   Checkcode           : 000000000000
   VendorID            : HWTC
   Ont Version         : MA5633 VER.A
   Ont SoftwareVersion : V8R313 C10
   Ont EquipmentID     : 5633
   Ont autofind time   : 2013-09-25 20:42:45+08:00
   ------------------------------------------------------------
huawei(config-if-gpon-0/3)#ont confirm 1 ontid 1 sn-auth 48575443E6D8B541 snmp
ont-lineprofile-id
 10 desc MA5633_0/3/1/1_lineprofile10
```


Copyright © Huawei Technologies Co., Ltd.

NOTE

If multiple D-CMTSs of the same type are connected to a port and the same line or service profile is bound to the D-CMTSs, add these D-CMTSs in batches by confirming the automatically discovered D-CMTSs in batches. This simplifies operations and improves configuration efficiency. To do so, change the preceding command huawei(config-if-gpon-0/3)#**ont confirm 1 ontid 1 sn-auth 48575443E6D8B541 snmp ont-lineprofile-id 10 desc MA5633_0/3/1/1_lineprofile10** to huawei(config-if-gpon-0/3)#**ont confirm 1 all sn-auth snmp ont-lineprofile-id 10 desc MA5633_0/3/1_lineprofile10**.

----End

Result

The D-CMTS is online.

After adding the D-CMTS, run the **display ont info** command to query the D-CMTS status. Ensure that **Control flag** is **active**, **Run State** is **online**, and **Config state** is **normal**.

```
huawei(config-if-gpon-0/3)#display ont info 1 1
  ------------------------------------------------------------------------
  F/S/P                : 0/3/1
  ONT-ID               : 1
  Control flag         : active    //The D-CMTS has been activated.
  Run state            : online    //The D-CMTS has been online.
  Config state         : normal    //The D-CMTS has been configured.
...//The following terminal display is omitted.
```

Follow-up Procedure

If the D-CMTS malfunctions, follow the troubleshooting suggestions listed in the following table to rectify faults.

D-CMTS Status	Troubleshooting Suggestion
The **Control flag** of the D-CMTS is **deactivated**.	In GPON port mode, run the **ont activate** command to activate the D-CMTS.
The D-CMTS is offline (**Run state** displayed as **offline**).	The physical line may be disconnected, or the optical module may be damaged. Rectify the fault by checking line connection and the hardware.
The D-CMTS fails to be configured (**Config state** displayed as **failed**)	The possible cause is that the D-CMTS cannot support the configured D-CMTS capability set. In this case, run the **display ont failed-configuration** command to query the failed configuration items and failure causes. Then rectify the fault accordingly.

16.4.2.8 Configuring a Management Channel Between an OLT and an MA5633

This section describes how to configure a management channel between an optical line terminal (OLT) and a distributed cable modem termination system (D-CMTS). After the configuration, you can log in to the D-CMTS from the OLT and configure the D-CMTS.

Copyright © Huawei Technologies Co., Ltd.

Data Plan

Item	Data	Remarks
Management VLAN and IP address of the OLT	ID of the management VLAN: 8 Type of the management VLAN: smart Management IP address: 192.168.50.1/24	To remotely log in to the D-CMTS from the OLT for configuration, ensure that the management VLAN of the OLT is the same as that of the D-CMTS and that the management IP address of the OLT is in the same network segment as that of the D-CMTS.
Management VLAN and IP address of the D-CMTS	ID of the management VLAN: 8 Type of the management VLAN: smart Management IP address: 192.168.50.2/24	

Procedure

Step 1 Configure a management channel between the OLT and the D-CMTS.

NOTE

Perform this operation only when the OLT remotely manages the D-CMTS through SNMP.

1. Set the inband management VLAN and IP address of the OLT.

   To remotely log in to the D-CMTS for configuration, set the inband management VLANs and IP addresses of the OLT and the D-CMTS on the OLT.

   ```
   huawei(config)#vlan 8 smart
   huawei(config)#port vlan 8 0/5 0
   huawei(config)#interface vlanif 8
   huawei(config-if-vlanif8)#ip address 192.168.50.1 24
   huawei(config-if-vlanif8)#quit
   ```

2. Set the inband management VLAN and IP address of the D-CMTS.

   Set the static IP address of the D-CMTS to 192.168.50.2/24, the IP address of the gateway to 192.168.50.1, and the ID of the management VLAN to 8 (the same as the management VLAN of the OLT).

   ```
   huawei(config)#interface gpon 0/3
   huawei(config-if-gpon-0/3)#ont ipconfig 1 1 static ip-address 192.168.50.2
   mask 255.255.255.0 gateway
       192.168.50.1 vlan 8
   huawei(config-if-gpon-0/3)#quit
   ```

3. Configure an inband management service flow.

   The following configurations are used as an example to configure an inband management service flow:

   - Configuration of the service flow:
     - ID of the management service flow: 0
     - ID of the management VLAN: 8

Copyright © Huawei Technologies Co., Ltd.

- ID of the GPON encapsulation mode (GEM) port: 0
- ID of the customer VLAN (C-VLAN): 8

- Device where upstream and downstream packet rates are limited: D-CMTS

  In this case, use the default traffic profile with ID 6, which does not limit the rate of a service flow. To limit packet rates, run the **traffic table ip** command to create a traffic profile and bind it to the service flow.

```
huawei(config)#service-port 0 vlan 8 gpon 0/3/1 ont 1 gemport 0 multi-service
user-vlan 8 rx-cttr 6 tx-cttr 6
```

NOTE

- On IPv6 networks, run the **dhcpv6-option permit-forwarding port 0/3/0 enable** command to enable DHCPv6 Option forwarding on a specified port.
- If CPEs support IPv6 prefixes, run the **security bind-route-nd enable** command to enable associated routes and neighbor entries. Then, the OLT automatically generates the routing and neighbor entries of a DHCPv6 user based on the user information recorded when the user goes online. This prevents the need of manually configuring static routes and sending neighbor discovery (ND) packets to the user side, thereby improving system security.

Step 2 Check whether the management channel between the OLT and the D-CMTS is available.

- Run the **ping *192.168.50.1*** command on the OLT to check whether the D-CMTS can communicate with the OLT. If the OLT can receive Internet Control Message Protocol (ICMP) ECHO-REPLY packets sent from the D-CMTS, the D-CMTS is connected to the OLT.
- Run the **telnet** command on the OLT to remotely log in to the ONU from the OLT to perform the configuration. The user name is root and the password is mduadmin.

----End

16.4.2.9 Configuring a Service Channel Between an OLT and a D-CMTS

Data Plan

Item	Data
L2VPN enterprise service	ID of the OLT VLAN (transparently transmitting D-CMTS packet tags): 200 ID of the D-CMTS VLAN: 200
Uplink ports	Port forwarding Dynamic Host Configuration Protocol (DHCP) and broadband packets: 0/4/0 Port forwarding cable modem (CM) management and VoD packets: 0/5/0

Procedure

- Configure a channel for the L2VPN enterprise service.
  1. Configure an L2VPN service VLAN (S-VLAN).

     The following configurations are used as an example to configure an S-VLAN:

Copyright © Huawei Technologies Co., Ltd.

- S-VLAN ID: 200
- S-VLAN type: smart
- ID of the VLAN containing uplink port 0/4/0: 200 (S-VLAN ID)

```
huawei(config)#vlan 200 smart
huawei(config)#port vlan 200 0/4 0
```

2. Configure a service flow to receive and transparently transmit D-CMTS packets.

   The following configurations are used as an example to configure a service flow:

   - Configuration of the service flow:
     - Service flow ID: 1
     - S-VLAN ID: 200
     - Customer VLAN (C-VLAN) ID: 200
   - Device where upstream and downstream packet rates are limited: D-CMTS

     In this case, use the default traffic profile with ID 6, which does not limit the rate of a service flow. To limit packet rates, run the **traffic table ip** command to create a traffic profile and bind it to the service flow.
   - C-VLAN and S-VLAN of the D-CMTS: same

```
huawei(config)#service-port 1 vlan 200 gpon 0/3/1 ont 1 gemport 1 multi-service
user-vlan 200 rx-cttr 6 tx-cttr 6
```

3. Configure the maximum number of dialup users allowed on a service port.

   For functions (such as, MAC address spoofing, anti-IP spoofing, anti-IPv6 spoofing, DHCP Proxy, IP Aware, IPoE single-MAC, VMAC DHCP aging, NS proxy response, ARP proxy response, DAD proxy, and DHCPv6 associated routes) depending on dialup operations performed by DHCP, DHCPv6, PPPoE, and SLAAC users, run this command to restrict the number of users allowed on each service port.

```
huawei(config)#security user max-user-count service-port 1 2048
```

- Configure a CM management channel.

  1. Configure a service flow to receive and transparently transmit D-CMTS packets.

     The following configurations are used as an example to configure service flows:

     - Configuration of a service flow:
       - S-VLAN ID: 100
       - C-VLAN ID: 100
     - Device where upstream and downstream packet rates are limited: D-CMTS

       In this case, use the default traffic profile with ID 6, which does not limit the rate of a service flow. To limit packet rates, run the **traffic table ip** command to create a traffic profile and bind it to the service flow.
     - C-VLAN and S-VLAN of the D-CMTS: same

```
huawei(config)#service-port vlan 100 gpon 0/3/1 ont 1 gemport 1 multi-service
user-vlan 200 rx-cttr 6 tx-cttr 6
```


Copyright © Huawei Technologies Co., Ltd.

NOTE

- On IPv6 networks, run the **dhcpv6-option permit-forwarding port 0/3/0 enable** command to enable DHCPv6 Option forwarding on a specified port.
- If CPEs support IPv6 prefixes, run the **security bind-route-nd enable** command to enable associated routes and neighbor entries. Then, the OLT automatically generates the routing and neighbor entries of a DHCPv6 user based on the user information recorded when the user goes online. This prevents the need of manually configuring static routes and sending neighbor discovery (ND) packets to the user side, thereby improving system security.

2. Configure the maximum number of dialup users allowed on a service port.

```
huawei(config)#security user max-user-count service-port 2 2048
```

----End

16.4.2.10 Configuring RF Port Parameters on an MA5633

Radio frequency (RF) port parameters define the frequency spectrum range for signal transmission and modulation mode. The configuration of RF port parameters implements data service transmission over cables.

Data Plan

Table 16-43 Data plan for RF port parameters

Item	Data
RF port	0/1/0
Upstream channels	● IDs: 1-4 ● Type: European standard (default channel type) ● ID of the upstream channel modulation profile: 1 (by default) ● Channel central frequency (MHz): 29.8, 42.60, 49.00, and 55.4
Downstream channels	● IDs: 1-16 ● Type: European standard (default channel type) ● Channel central frequency (MHz): 602.00, 610.00, 618.00, ..., and 722.00

Procedure

- Log in to and configure the ONU.

  You can remote log in to the ONU from the OLT to perform the configuration. The user name is **root** and the password is **mduadmin**.
- Customize RF port parameters in cable mode.
  1. Configure the frequency spectrum range and channel type.

     In this example, the channel is of the European type. To change the type to North American, run the **cable** command.
  2. Configure RF port parameters for upstream channels and activate the upstream channels.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
frequency and **channel-width**	A central frequency and a frequency bandwidth determine a frequency range, within which packets are transmitted. For example, the central frequency of a European channel is 55 MHz and the frequency bandwidth is 6400 kHz. Then the frequency range of the channel is 51.8-58.2 MHz.
modulation-profile	An upstream channel modulation profile defines parameters for processing the signals transmitted over the upstream channel. You do not need to configure an upstream channel modulation profile generally. Ports automatically bind to profile 1 by default.

The following configurations are used as an example to configure RF port parameters:

- Number of upstream channels: 4
- Frequency bandwidth of the channels: 3.2 MHz (default value)

```
huawei(config)#interface cable 0/1/0
huawei(config-if-cable-0/1/0)#cable upstream 1 frequency 29.8 enable
huawei(config-if-cable-0/1/0)#cable upstream 2 frequency 42.60 enable
huawei(config-if-cable-0/1/0)#cable upstream 3 frequency 49.00 enable
huawei(config-if-cable-0/1/0)#cable upstream 4 frequency 55.40 enable
```

3. Configure RF port parameters for downstream channels and activate the downstream channels.

Parameter	Description
modulation	A greater modulation mode value for downstream channels results in a higher channel bandwidth but weaker anti-interference capability. Therefore, configure the modulation mode based on site requirements. The default modulation mode is QAM256. This example uses the default setting.

The following configuration is used as an example to configure RF parameters for downstream channels: A total of 16 downstream channels have been purchased.

```
huawei(config-if-cable-0/1/0)#cable downstream 1 frequency 602.00 enable
huawei(config-if-cable-0/1/0)#cable downstream 2 frequency 610.00 enable
huawei(config-if-cable-0/1/0)#cable downstream 3 frequency 618.00 enable
huawei(config-if-cable-0/1/0)#cable downstream 4 frequency 626.00 enable
huawei(config-if-cable-0/1/0)#cable downstream 5 frequency 634.00 enable
huawei(config-if-cable-0/1/0)#cable downstream 6 frequency 642.00 enable
huawei(config-if-cable-0/1/0)#cable downstream 7 frequency 650.00 enable
```


Copyright © Huawei Technologies Co., Ltd.

```
huawei(config-if-cable-0/1/0)#cable downstream 8 frequency 658.00 enable
huawei(config-if-cable-0/1/0)#cable downstream 9 frequency 666.00 enable
huawei(config-if-cable-0/1/0)#cable downstream 10 frequency 674.00 enable
huawei(config-if-cable-0/1/0)#cable downstream 11 frequency 682.00 enable
huawei(config-if-cable-0/1/0)#cable downstream 12 frequency 690.00 enable
huawei(config-if-cable-0/1/0)#cable downstream 13 frequency 698.00 enable
huawei(config-if-cable-0/1/0)#cable downstream 14 frequency 706.00 enable
huawei(config-if-cable-0/1/0)#cable downstream 15 frequency 714.00 enable
huawei(config-if-cable-0/1/0)#cable downstream 16 frequency 722.00 enable
```

----End

Result

1. The transmit power of the downstream channels meets site requirements.

   Run the **display cable downstream** *frameid/slotid/portid* { **all** | *channel-id* } **status** command to check whether the RF port parameters meet site requirements.

2. The signal-to-noise (SNR) ratio of the upstream channels meets site requirements.

   Run the **display cable signal quality** [*frameid/slotid/portid* [**upstream** *channel-id*]] command to check whether the RF port parameters meet site requirements. A greater SNR ratio results in better signal quality. The recommended SNR ratio is greater than 30 dB.

16.4.2.11 Configuring the L2VPN Enterprise Service on an MA5633

In the upstream direction, a cable modem (CM) connects to a distributed cable modem termination system (D-CMTS) through a cable. In the downstream direction, the CM connects to a switch to provide the L2VPN enterprise service to the users connected to the switch.

Context

An L2VPN S-VLAN can be configured through a CM configuration file or commands. Only one mode is used each time generally. If both modes are used, the S-VLAN configuration through commands preferentially takes effect on the system when the CM goes online.

- S-VLAN configuration through a CM configuration file: Run the **vlan** command to add a CM S-VLAN and run the **port vlan** command to add the uplink port for the CM to the S-VLAN. Then, run the **cable service-vlan** command to make the CM go online. The L2VPN S-VLAN is specified in the CM configuration file. When the CM goes online, the system obtains the L2VPN S-VLAN from the CM configuration file and automatically creates L2VPN service flows.
- S-VLAN configuration through commands: Manually configure the L2VPN S-VLAN on the system. For details, see the following procedure.

Data Plan

Table 16-44 Data plan for the L2VPN service

Item	Data
VLAN	ID of the L2VPN S-VLAN: 200; type of the VLAN: smart
Uplink port	0/0/1

Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Log in to and configure the ONU.

You can remote log in to the ONU from the OLT to perform the configuration. The user name is **root** and the password is **mduadmin**.

Step 2 Configure a CM management S-VLAN.

The ID of the CM management S-VLAN is 100 and the type of the VLAN is smart.

```
huawei(config)#vlan 100 smart
huawei(config)#port vlan 100 0/0 1
huawei(config)#cable service-vlan 100     //The CM S-VLAN identifies a CM service
flow. After the CM S-VLAN is configured, the D-CMTS automatically creates a service
flow when the CM goes online.
  Info: The new service VLAN will take effect after the CM is restarted, are you
 sure to modify? (y/n)[n]:y
```

Step 3 Create an L2VPN S-VLAN and add the uplink port to it.

The ID of the L2VPN S-VLAN is 200 and the type of the VLAN is smart. Uplink port 0/0/1 is added to S-VLAN 200.

When the L2VPN S-VLAN is configured through commands, the ID of the L2VPN VLAN is 200 for the CM with MAC address 0000-0000-1111 connected to port 0/1/0.

- To configure the L2VPN S-VLAN through a CM configuration file, run the following commands:
  ```
  huawei(config)#vlan 200 smart
  huawei(config)#port vlan 200 0/0 1
  ```
- To configure the L2VPN S-VLAN through commands, run the following commands:
  ```
  huawei(config)#vlan 200 smart
  huawei(config)#cable l2vpn dot1q 0/1/0 cm 0000-0000-1111 200
  huawei(config)#port vlan 200 0/0 1
  ```

----End

16.4.2.12 Verifying Services

A distributed cable modem termination system (D-CMTS) locates on an optical node when the D-CMTS functions as a standalone NE. To facilitate service verification, the D-CMTS supports multiple remote service verification methods, such as Dynamic Host Configuration Protocol (DHCP) dialup emulation tests. This allows commissioning and configuration engineers to remotely verify services. In addition, this section describes how to verify the L2VPN service on site.

Prerequisites

- The D-CMTS is properly connected to the upper-layer network.
- The DHCP server, Trivial File Transfer Protocol (TFTP) server, and softswitch or IP multimedia subsystem (IMS) have been configured.

Procedure

- Log in to and configure the ONU.

Copyright © Huawei Technologies Co., Ltd.

You can remote log in to the ONU from the OLT to perform the configuration. The user name is **root** and the password is **mduadmin**.

- Perform a DHCP dialup emulation test.

  In this test, a cable modem (CM) is emulated on the MA5633 to apply to the DHCP server for an IP address. This checks whether the MA5633 can communicate with the DHCP server and verifies CM DHCP configurations on the DHCP relay, proxy, and server.

  1. Run the **simulate dhcp start cm** *mac-address* [**option60** *option60*] command to start a DHCP dialup emulation test.

     NOTE

     You can run the **simulate dhcp stop** command to stop the DHCP emulation.

  2. Run the **display simulation dhcp** command to query the results of the DHCP dialup emulation test.
  3. Check whether the **User IP** has obtained an IP address.

- Check the CM status.

  Run the **display cable modem** command to query the CM status in **Status**.

```
huawei(config)#display cable modem  all

------------------------------------------------------------------------------
-
 Idx   MAC            IP              I/F          Status   Prim  Num Ver  DS
RX
                                                           SID   CPE
Power

------------------------------------------------------------------------------
-
 1     0023-ED6F-21A3 192.168.1.118   1/1/0/U4     ol-pt    1     0   D2.0
-

------------------------------------------------------------------------------
-
 Total:
1
 ol: 0, ol-ptd: 0, ol-pt: 1, ol-d: 0, wol: 0, wol-ptd: 0, wol-pt: 0, wol-d:
0,
pol: 0, pol-ptd: 0, pol-pt: 0, pol-d: 0, offline: 0, rej-m: 0, rej-pt: 0, rej-
o:
 0, init: 0, init-rc: 0, DHCP: 0, DHCP-O: 0, DHCP-R: 0, DHCP-C: 0, REG:
0
 Note: 1. Idx is the index of a
CM.
       2. The downstream received power is in the unit of
dBmV.
       3. In status, "ol" means online, "rej" means reject.
```

  The following table lists the CM status and handling suggestions.

CM Status	Description	Handling Suggestion
init	Indicates that the CM initialization ranging message is received.the CM initialization.	If a CM is always in the ranging state, the ranging fails. Then check radio frequency (RF) line indicators and detect line faults.

Copyright © Huawei Technologies Co., Ltd.

CM Status	Description	Handling Suggestion
init-rc	Indicates that the CM initialization ranging is complete.	No action is required. The ranging of the CM is complete.
DHCP	Indicates that the DHCP discovery from the CM is received.	If a CM initiates a DHCP request but does not obtain an IP address, check the DHCP server, routing between the OLT and the DHCP server, and DHCP server parameter settings.
● DHCP-O ● DHCP-R ● DHCP-C	● DHCP-O: indicates that the offer from the DHCP server is received. ● DHCP-R: indicates that the DHCP request from the CM is received. ● DHCP-C: indicates that the acknowledge from the DHCP server is received.	The DHCP server has assigned an IP address to the CM and sent configuration file name and IP address of the TFTP or ToD server to the CM using the Option 67 and Option 66 fields (the Option 67 field carries the configuration file name and the Option 66 field carries the IP address of the TFTP or ToD server). If the CM is always in the DHCP-C state, the CM fails to obtain the configuration file. Then check the TFTP server, routing between the OLT and the TFTP server, and TFTP server parameter settings.
REG	Indicates that a registration is started.	If the CM is always in the register state, the CM obtains an incorrect configuration file. Then change the configuration file.

Copyright © Huawei Technologies Co., Ltd.

CM Status	Description	Handling Suggestion
● ol ● ol-pt ● ol-ptd ● ol-d ● wol ● wol-pt ● wol-ptd ● wol-d ● pol ● pol-pt ● pol-ptd	● ol: indicates that the CM is online. (valid only for CMs complying with DOCSIS 2.0) ● ol-pt: indicates that the CM is online and passes the BPI authentication. (valid only for CMs complying with DOCSIS 2.0) ● ol-ptd: indicates that the CM is online and passes the BPI authentication, and NetAccessEnable is disabled. (valid only for CMs complying with DOCSIS 2.0) ● ol-d: indicates that the CM is online and NetAccessEnable is disabled. (valid only for CMs complying with DOCSIS 2.0) ● wol: indicates that the CM is online and all channels bound to the CM are available. (valid only for CMs complying with DOCSIS 3.0) ● wol-pt: indicates that the CM is online and passes the BPI authentication, and all channels bound to the CM are available. (valid only for CMs complying with DOCSIS 3.0) ● wol-ptd: indicates that the CM is online and passes the BPI authentication, NetAccessEnable is disabled, and all channels bound to the CM are available. (valid only for CMs complying with DOCSIS 3.0) ● wol-d: indicates that the CM is online, NetAccessEnable is disabled, and all channels bound to the CM are available. (valid only for CMs complying with DOCSIS 3.0) ● pol: indicates that the CM is online and some channels	No action is required. The status indicates that the CM has registered

Copyright © Huawei Technologies Co., Ltd.

CM Status	Description	Handling Suggestion
● pol-d	bound to the CM are available. (valid only for CMs complying with DOCSIS 3.0) ● pol-pt: indicates that the CM is online and passes the BPI authentication, and some channels bound to the CM are available. (valid only for CMs complying with DOCSIS 3.0) ● pol-ptd: indicates that the CM is online and passes the BPI authentication, NetAccessEnable is disabled, and some channels bound to the CM are available. (valid only for CMs complying with DOCSIS 3.0) ● pol-d: indicates that the CM is online, NetAccessEnable is disabled, and some channels bound to the CM are available. (valid only for CMs complying with DOCSIS 3.0)	with the OLT and can correctly transmit and receive services.
offline	Indicates the offline status.	If the CM is in the offline state, check the power status, noise, and channel frequency of the CM.
● rej-m ● rej-pt ● rej-o	● rej-m: indicates that the MIC verification fails. ● rej-pt: indicates that the BPI authentication fails. ● rej-o: indicates that the authentication reject due to other reasons.	If the CM is in the reject state, no service flow can be created. Then check the CM authentication and CM message integrity check (MIC), and check whether class of service (COS) parameters specified in the CM configuration file are supported by the OLT.

- Verify that the L2VPN service can be provisioned.

  After the CM is installed in the enterprise and the switch connected to the CM is commissioned, L2VPN service can be provisioned.

----End

16.4.3 WLAN Hotspot Radio Backhaul Service Networking

In wireless local area network (WLAN) hotspot radio backhaul service networking, an MA5633 connects to cable modems (CMs) through radio frequency (RF) ports. A CM connects to wireless

Copyright © Huawei Technologies Co., Ltd.

access points (APs) to provide wireless fidelity (Wi-Fi) access for users. This section describes how to configure the MA5633 to provision the WLAN hotspot radio backhaul service.

Service Requirements

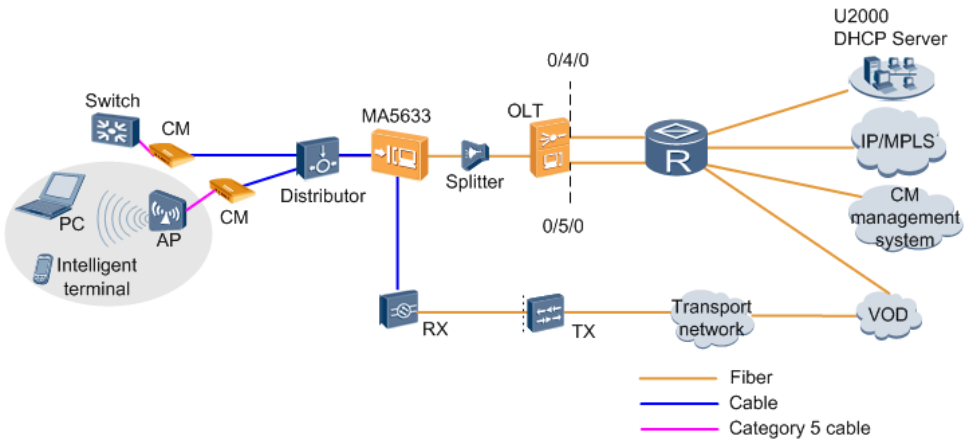
A network supplier needs to provide the Internet access service through Wi-Fi for a business area covered by APs.

Usage Scenario

As shown in **Figure 16-13**, an MA5633 is deployed on an optical node and CMs are deployed at shops. The CMs connect to RF ports on the MA5633 through cables.

- A CM connects to wireless APs to provide the WLAN hotspot radio backhaul service. The wireless APs provide Wi-Fi access for users.
- Wi-Fi users access the Internet through Dynamic Host Configuration Protocol (DHCP) dialup.

Figure 16-13 WLAN hotspot radio backhaul service networking



Configuration

The method of configuring the WLAN hotspot radio backhaul service is the same as that of configuring the L2VPN enterprise service and therefore is not described in this section. For details, see **16.4.2.2 Configuration Process**.

Copyright © Huawei Technologies Co., Ltd.

17 Electrical Service Configuration

About This Chapter

The MA5621/MA5621A can be used for remote and intelligent information collection and transmission (regarding power stations and user electricity consumption) in an electricity system, and can also be used for video monitoring.

17.1 Configuration Example of the FTTx Service (GPON Access)
This topic describes how to configure the data service in the GPON access mode in various FTTx scenarios.

Copyright © Huawei Technologies Co., Ltd.

17.1 Configuration Example of the FTTx Service (GPON Access)

This topic describes how to configure the data service in the GPON access mode in various FTTx scenarios.

17.1.1 Configuration Example of Transmitting Video Monitoring Data over Ethernet Access

An optical network unit (ONU) can receive video monitoring data through gigabit Ethernet (GE)/fast Ethernet (FE) autonegotiation electrical ports and transmit the data to the optical line terminal (OLT) through gigabit-capable passive optical network (GPON) ports. Then the OLT transmits the data to an upper-layer device.

Service Requirements

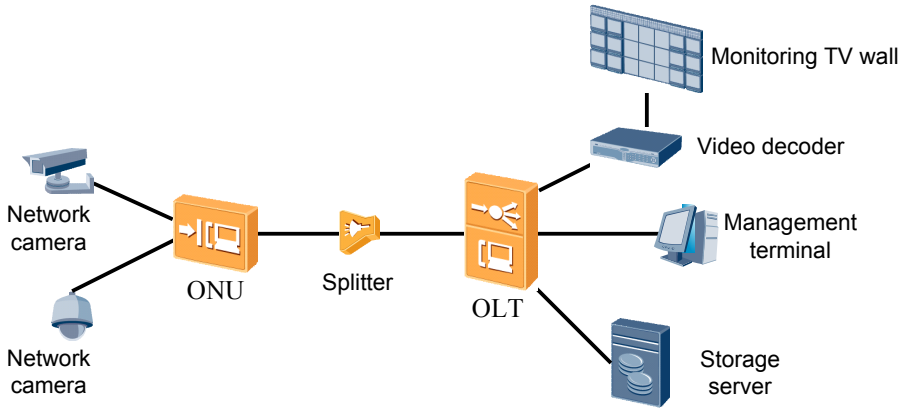
- To enhance area security, a video monitoring point is deployed and monitored in real time at the monitoring center.
- The video encoder at this monitoring point provides Ethernet access so an ONU can receive video monitoring data over Ethernet.
- The data is transmitted over a GPON network.

Networking

Figure 17-1 shows an example network for configuring video monitoring data transmission over Ethernet.

- Located at a monitored point, the ONU is connected to video encoders through GE/FE autonegotiation electrical ports. The ONU receives encoded video monitoring information and forwards the information upstream to an OLT at the monitoring center.
- The OLT forwards the information to other monitoring devices at the monitoring center.

Figure 17-1 Example network for configuring video monitoring data transmission over Ethernet



NOTE

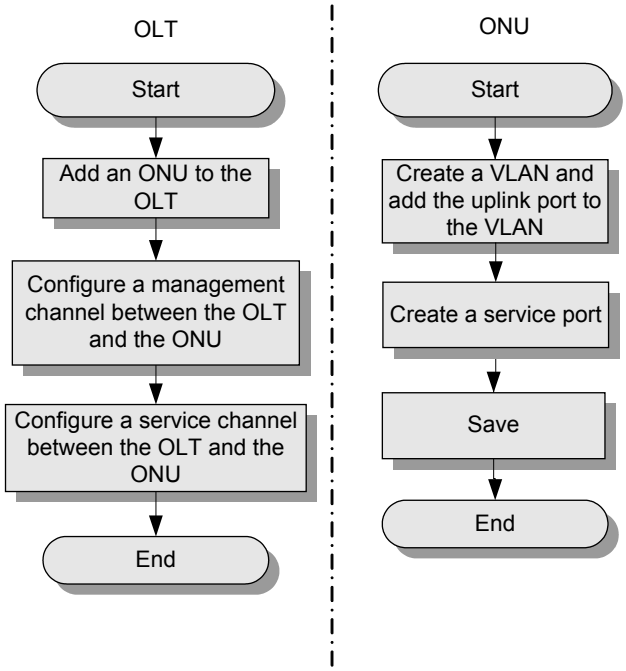
In this example, an MA5621 is used as the ONU.

Copyright © Huawei Technologies Co., Ltd.

Configuration Flowchart

Figure 17-2 provides the procedure for configuring video monitoring data transmission over Ethernet.

Figure 17-2 Procedure for configuring video monitoring data transmission over Ethernet



Device	Step	Remarks
OLT	1. Add an ONU on the OLT.	You can configure data for an ONU only after it has been added on an OLT.
	2. Configure a management channel between the OLT and the ONU.	After configuring an inband management channel between the OLT and the ONU, you can log in to the ONU and configure data for the ONU on the OLT.
	3. Configure a service channel between the OLT and the ONU.	The video monitoring data is received by the ONU and then transmitted to the OLT. The OLT transparently transmits the data to the monitoring center over the upper-layer network.
ONU	1. Configure the virtual local area network (VLAN) uplink port.	To transmit packets with a VLAN tag through an uplink port, add the uplink port to the VLAN.

Copyright © Huawei Technologies Co., Ltd.

Device	Step	Remarks
	2. Configure a service port.	Create a service port on the ONU to receive the video monitoring data. The data is transmitted upstream to the OLT through an uplink port.

Data Plan

Table 17-1 provides the OLT data plan, and Table 17-2 provides the ONU data plan.

Table 17-1 Data plan for configuring video monitoring data transmission over Ethernet-OLT side

Item	Data
VLAN	● Uplink port: 0/19/0 ● Inband management VLAN: smart VLAN 8 ● Service VLAN: smart VLAN 100
Inband management IP address	192.168.50.20/24
GPON service board	● Port: 0/3/1 ● ONU ID: 1 ● ONU authentication mode: SN ● ONU SN: 48575443E6D8B541
DBA profile	● Profile name: VideoMonitoring ● Type: type3 ● Assured bandwidth: 20 Mbit/s ● Maximum bandwidth: 50 Mbit/s
ONU line profile	● Profile ID: 10, bound to DBA profile VideoMonitoring ● GEM port ID: 0 (used for transmitting inband management service stream) ● GEM port ID: 1 (used for transparently transmitting video monitoring service stream) ● T-CONT ID: 5
ONU management mode	SNMP

Copyright © Huawei Technologies Co., Ltd.

Table 17-2 Data plan for configuring video monitoring data transmission over Ethernet-ONU side

Configuration Item	Data	Remarks
Inband management IP address	192.168.50.2/24	-
Traffic profile	Index 6 (default)	-
Service port	0/1/1	-
Uplink port	0/0/0	-
Uplink VLAN	smart VLAN 100	The uplink VLAN must be the same as the user VLAN on the OLT.
User VLAN	smart VLAN 2	-

Procedure

Step 1 Configure the OLT.

1. Create an SVLAN and add an upstream port to it.

   Create smart VLAN 100, and then add upstream port 0/19/0 to the VLAN.

   ```
   huawei(config)#vlan 100 smart
   huawei(config)#port vlan 100 0/19 0
   ```

2. (Optional) Configure upstream link aggregation.

   In this example, a single uplink port is used. In the case of multiple uplink ports, upstream link aggregation can be configured.

3. Configure GPON ONU profiles.

   GPON ONU profiles include the DBA profile, line profile, service profile, and alarm profile.

   - DBA profile: A DBA profile describes the GPON traffic parameters. A T-CONT is bound to a DBA profile for dynamic bandwidth allocation, improving the upstream bandwidth usage rate.
   - Line profile: A line profile describes the binding between the T-CONT and the DBA profile, the QoS mode of the traffic stream, and the mapping between the GEM port and the ONU-side service.
   - Service profile: A service profile provides the service configuration channel for the ONU that is managed through OMCI.
   - Alarm profile: An alarm profile contains a series of alarm thresholds to measure and monitor the performance of activated ONU lines. When a statistical value reaches the threshold, the host is notified and an alarm is reported to the log host and the NMS.

Copyright © Huawei Technologies Co., Ltd.

a. Add a DBA profile.

You can at first run the **display dba-profile** command to query the DBA profiles existing in the system. If the DBA profiles existing in the system do not meet the requirements, you need to run the **dba-profile add** command to add a DBA profile.

Configure the profile name to VideoMonitoring, profile type to Type3, assured bandwidth to 20 Mbit/s, and maximum bandwidth to 50 Mbit/s.

```
huawei(config)#dba-profile add profile-name VideoMonitoring type3 assure
20480 max 51200
```

b. Add an ONU line profile.

Add GPON ONU line profile 10 and bind T-CONT 5 to the DBA profile named VideoMonitoring. In this way, the T-CONT can provide flexible DBA solutions based on different configurations in the DBA profile.

```
huawei(config)#ont-lineprofile gpon profile-id 10
huawei(config-gpon-lineprofile-10)#tcont 5 dba-profile-name
VideoMonitoring
```

Add GEM port 0 for transmitting management traffic streams, GEM port 1 for transmitting video monitoring information traffic streams. Bind GEM port 0 and GEM port 1 to T-CONT 5. Configure the QoS mode to priority-queue (default) and the queue priority to 3.

```
huawei(config-gpon-lineprofile-10)#gem add 0 eth tcont 5 priority-queue 3
huawei(config-gpon-lineprofile-10)#gem add 1 eth tcont 5 priority-queue 3
```

Configure the mapping mode from the GEM port to ONU-side service to VLAN (default), map the service port of management VLAN 8 to GEM port 0, map the service port of video monitoring information SVLAN 100 to GEM port 1.

```
huawei(config-gpon-lineprofile-10)#mapping-mode vlan
huawei(config-gpon-lineprofile-10)#gem mapping 0 0 vlan 8
huawei(config-gpon-lineprofile-10)#gem mapping 1 1 vlan 100
```

After the configuration is complete, run the **commit** command to make the configured parameters take effect.

```
huawei(config-gpon-lineprofile-10)#commit
huawei(config-gpon-lineprofile-10)#quit
```

c. (Optional) Add an alarm profile.

- The ID of the default GPON alarm profile is 1. The thresholds of all the alarm parameters in the default alarm profile are 0, which indicates that no alarm is generated.
- In this example, the default alarm profile is used, and therefore the configuration of the alarm profile is not required.
- Run the **gpon alarm-profile add** command to add an alarm profile, which is used for monitoring the performance of an activated ONU line.

4. Add an ONU on the OLT.

The ONU is connected to the GPON port of the OLT through an optical fiber. You can perform the service configuration only after adding an ONU successfully on the OLT.

a. Add an ONU.

Connect the ONU to GPON port 0/3/1. The ONU ID is 1, the SN is 48575443E6D8B541, the management mode is SNMP, and the bound line profile ID is 10.

There are two ways to add an ONU. Select either of the two ways according to actual conditions.

Copyright © Huawei Technologies Co., Ltd.

- Add an ONU offline: If the password or SN of an ONU is obtained, you can run the **ont add** command to add the ONU offline.
- Automatically find an ONU: If the password or SN of an ONU is unknown, run the port ont-auto-find command in the GPON mode to enable the ONU auto-find function of the GPON port. Then, run the **ont confirm** command to confirm the ONU.

To add an ONU offline, do as follows:

```
huawei(config)#interface gpon 0/3
huawei(config-if-gpon-0/3)#ont add 1 1 sn-auth 48575443E6D8B541 snmp ont-
lineprofile-id
 10 desc MA5621_0/3/1/1_lineprofile10
```

To automatically find an ONU, do as follows:

```
huawei(config)#interface gpon 0/3
huawei(config-if-gpon-0/3)#port 1 ont-auto-find enable
huawei(config-if-gpon-0/3)#display ont autofind 1
   //After this command is executed, the information about all ONUs
connected to
  //the GPON port through the optical splitter is displayed.

   ------------------------------------------------------------
   Number              : 1
   F/S/P               : 0/3/1
   Ont SN              : 48575443E6D8B541
   Password            :
   VenderID            : HWTC
   Ont Version         : MA5621
   Ont SoftwareVersion : V800R310C00
   Ont EquipmentID     : SmartAX MA5621
   Ont autofind time   : 2011-09-10 11:20:16
   ------------------------------------------------------------
huawei(config-if-gpon-0/3)#ont confirm 1 ontid 1 sn-auth 48575443E6D8B541
snmp ont-lineprofile-id
 10 desc MA5621_0/3/1/1_lineprofile10
```

NOTE

If multiple ONUs of the same type are connected to a port and the same line profile or service profile is bound to the ONUs, you can add ONUs in batches by confirming the auto-found ONUs in batches to simplify the operation and increase the configuration efficiency. For example, the preceding command can be modified as follows:

huawei(config-if-gpon-0/3)#**ont confirm 1 all sn-auth snmp ont-lineprofile-id 10 desc MA5621_0/3/1_lineprofile10**.

5. Confirm that the ONU goes online normally.

   After an ONU is added, run the **display ont info** command to query the current status of the ONU. Ensure that **Control flag** of the ONU is **active**, **Run State** is **online**, **Config state** is **normal**, and **Match state** is **match**.

```
huawei(config-if-gpon-0/3)#display ont info 1 1

------------------------------------------------------------------------
  F/S/P                :
0/3/1
  ONT-ID               :
1
  Control flag         : active    //Indicates that the ONU is
activated.
  Run state           : online    //Indicates that the ONU already goes online
normally.
  Config state         : normal    //Indicates that the configuration status
of the ONU is normal.
```


Copyright © Huawei Technologies Co., Ltd.

```
  Match state         : match     //Indicates that the capability profile bound
to the ONU is
                                        //consistent with the actual capability
of the ONU.
...//The rest of the response information is omitted.

huawei(config-if-gpon-0/3)#quit
```

If the ONU state fails, the ONU fails to be in the up state, or the ONU does not match, check the ONU state by referring to the above-mentioned descriptions.

- If **Control flag** is **deactive**, run the **ont activate** command in the GPON port mode to activate the ONU.
- If the ONU fails to be in the up state, that is, **Run state** is **offline**, the physical line may be broken or the optical transceiver may be damaged. You need to check both the material and the line.
- If the ONU state fails, that is, **Config state** is **failed**, the ONU capability set outmatches the actual ONU capabilities. In this case, run the **display ont failed-configuration** command in the diagnosis mode to check the failed configuration item and the failure cause. Then, rectify the fault according to actual conditions.

  NOTE

  If an ONT supports only four queues, the values of 4-7 of the priority-queue parameter in the gem add command are invalid. After configuration recovers, Config state will be failed.

6. Configure the management channel from the OLT to the ONU.

   NOTE

   Only when the OLT remotely manages the ONU through SNMP, the management channel needs to be configured. When the OLT remotely manages the ONU through OMCI, the management channel need not be configured.

   a. Configure the inband management VLAN and IP address of the OLT.

      To log in to the ONU through Telnet and configure the ONU from the OLT, you must configure the inband management VLANs and IP addresses of the OLT and the ONU on the OLT.

      Create management VLAN 8 and add upstream port 0/0/0 to it. Configure the inband management IP address to 192.168.50.20/24.

      ```
      huawei(config)#vlan 8 smart
      huawei(config)#port vlan 8 0/19 0
      huawei(config)#interface vlanif 8
      huawei(config-if-vlanif8)#ip address 192.168.50.20 24
      huawei(config-if-vlanif8)#quit
      ```

   b. Configure the inband management VLAN and IP address of the ONU.

      Configure the static IP address of the ONU to 192.168.50.2/24 and the management VLAN ID to 8 (the same as the management VLAN of the OLT).

      ```
      huawei(config)#interface gpon 0/3
      huawei(config-if-gpon-0/3)#ont ipconfig 1 1 ip-address 192.168.50.2 mask
      255.255.255.0 manage-vlan 8
      ```

   c. Configure an inband management service port.

      Configure the management service port ID to 0, management VLAN ID to 8, GEM port ID to 0, and CVLAN ID to 8. The rate of the inband service port on the OLT is not limited. Therefore, use traffic profile 6 (default). To limit the rate of the service port, run the **traffic table ip** command to add a traffic profile and bind it to the service port.

Copyright © Huawei Technologies Co., Ltd.

```
huawei(config)#service-port 0 vlan 8 gpon 0/3/1 ont 1 gemport 0 multi-
service
user-vlan 8 rx-cttr 6 tx-cttr 6
```

7. Confirm that the management channel between the OLT and the ONU is available.
   - On the OLT, run the **ping *192.168.50.2*** command to check the connectivity to the ONU. The ICMP ECHO-REPLY packet from the ONU should be received.
   - You can run the **telnet *192.168.50.2*** command to telnet to the ONU and then configure the ONU.
8. Create a service port.

   Configure the Video Monitoring Data service port ID to 1, SVLAN ID to 100, GEM port ID to 1, CVLAN ID to 100. Rate limitation for upstream and downstream packets is performed on the ONU instead of on the OLT. Therefore, use traffic profile 6 (default). To limit the rate of the service port, run the **traffic table ip** command to add a traffic profile and bind it to the service port.

   The CVLAN must be the same as the upstream VLAN of the ONU.

   ```
   huawei(config)#service-port 1 vlan 100 gpon 0/3/1 ont 1 gemport 1 multi-
   service
   user-vlan 100 rx-cttr 6 tx-cttr 6
   ```
9. Configure queue scheduling.

   Use the 3PQ+5WRR queue scheduling. Queues 0-4 adopt the WRR mode, with the weights of 10, 10, 20, 20, and 40 respectively; queues 5-7 adopt the PQ mode.

   Queue scheduling is a global configuration. You need to configure queue scheduling only once on the OLT, and then the configuration takes effect globally. In the subsequent phases, you need not configure queue scheduling repeatedly when configuring other services.

   ```
   huawei(config)#queue-scheduler wrr 10 10 20 20 40 0 0 0
   ```

   Configure the mapping between queues and 802.1p priorities. Priorities 0-7 map queues 0-7 respectively.

   For the service board that supports only four queues, the mapping between 802.1p priorities and queue IDs is as follows: priorities 0 and 1 map queue 1; priorities 2 and 3 map queue 2; priorities 4 and 5 map queue 3; priorities 6 and 7 map queue 4.

   ```
   huawei(config)#cos-queue-map cos0 0 cos1 1 cos2 2 cos3 3 cos4 4 cos5 5 cos6 6
   cos7 7
   ```
10. Save the data.

    ```
    huawei(config)#save
    ```

Step 2 Configure the ONU.

NOTE

Because the management VLAN and the management IP address have been configured, you can run the **telnet *192.168.50.2*** command on the OLT to log in to the ONU to perform the configuration. You can also log in to the ONU through a serial port to perform the configuration.

1. Log in to the ONU to perform the configuration.

   On the OLT, use the management IP address of the ONU to log in to the ONU through Telnet. User name: **root** (default). Password: **mduadmin** (default).

   ```
   huawei(config)#telnet 192.168.50.2
   { <cr>|service-port<U><0,4294967295> }:

     Command:
   ```


Copyright © Huawei Technologies Co., Ltd.

```
          telnet 192.168.50.2
  Press CTRL_] to quit telnet mode
  Trying 192.168.50.2 ...
  Connected to 192.168.50.2 ...
>>User name:root
>>User password:       //It is not displayed on the console.
```

2. Create a VLAN.

   ```
   huawei(config)#vlan 100 smart
   ```

3. Add an uplink port to the VLAN.

   Add uplink port 0/0/0 to the VLAN.

   ```
   huawei(config)#port vlan 100 0/0 0
   ```

4. Create a service port.

   Create service port 2. Its user VLAN ID is 2 and service VLAN ID is 100. Use the default traffic profile (traffic profile 6). To limit the traffic rate, run the **traffic table ip** command to configure the traffic profile.

   ```
   huawei(config)#service-port 2 vlan 100 eth 0/1/1 multi-service user-vlan 2 rx-
   cttr 6
   tx-cttr 6
   ```

5. Save the data.

   ```
   huawei(config)#save
   ```

----End

Result

After the preceding configurations are complete, devices at the monitoring center (such as the storage server, management terminal, and video decoder) will receive video monitoring information.

Configuration File

Configure the OLT.

```
vlan 100 smart
port vlan 100 0/19 0
vlan 8 smart
port vlan 8 0/19 0
interface vlanif 8
ip address 192.168.50.20 24
quit
dba-profile add profile-name VideoMonitoring type3 assure 20480 max 51200
ont-lineprofile gpon profile-id 10
tcont 5 dba-profile-name VideoMonitoring
gem add 0 eth tcont 5 priority-queue 3
gem add 1 eth tcont 5 priority-queue 3
mapping-mode vlan
gem mapping 0 0 vlan 8
gem mapping 1 1 vlan 100
commit
quit
interface gpon 0/3
port 1 ont-auto-find enable
display ont autofind 1
ont confirm 1 ontid 1 sn-auth 48575443E6D8B541 snmp ont-lineprofile-id
 10 desc MA5621_0/3/1/1_lineprofile10
ont ipconfig 1 1 static ip-address 192.168.50.2 mask 255.255.255.0 vlan 8
```


Copyright © Huawei Technologies Co., Ltd.

```
ont alarm-profile 1 1 profile-id 1
service-port 0 vlan 8 gpon 0/3/1 ont 1 gemport 0 multi-service
user-vlan 8 rx-cttr 6 tx-cttr 6
service-port 1 vlan 100 gpon 0/3/1 ont 1 gemport 1 multi-service
user-vlan 100 rx-cttr 6 tx-cttr 6
queue-scheduler wrr 10 10 20 20 40 0 0 0
cos-queue-map cos0 0 cos1 1 cos2 2 cos3 3 cos4 4 cos5 5 cos6 6 cos7 7
save
```

Configure the ONU.

```
vlan 100 smart
port vlan 100 0/0 0
service-port 2 vlan 100 eth 0/1/1 multi-service user-vlan 2 rx-cttr 6 tx-cttr 6
save
```

17.1.2 Configuration Example of Intelligently Collecting Power Consumption Information over Ethernet Access

An optical network unit (ONU) can intelligently collect power consumption information in the electrical power system through gigabit Ethernet (GE)/fast Ethernet (FE) autonegotiation electrical ports, and transmit the data upstream to the optical line terminal (OLT) through gigabit-capable passive optical network (GPON) ports.

Service Requirements

- A large number of power consumption information in the electrical power system needs to be collected in real time and transmitted to an automatic meter reading system (AMR) server.
- The smart meter on the user side has a serial port and an ONU is connected to the smart meter through the serial port.
- The power consumption information is transmitted through a GPON network.

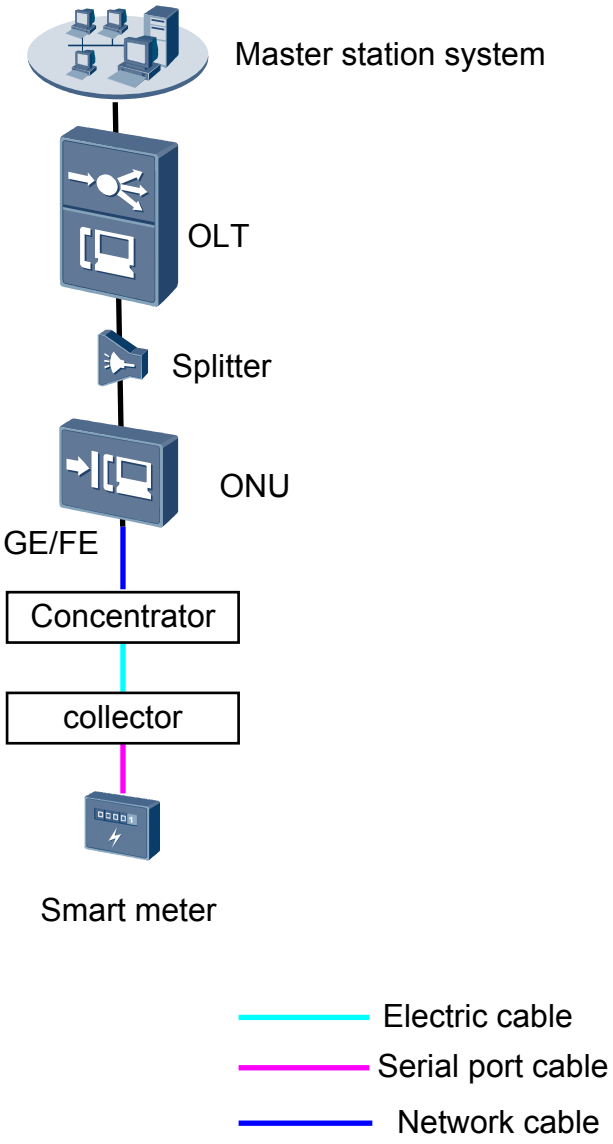
Networking

Figure 17-3 shows an example network for configuring intelligent collection of power consumption information in the electrical power system over Ethernet.

- The ONU is connected to a concentrator through a GE/FE autonegotiation electrical port. The concentrator is connected to a collector using power cables and sends the power consumption information collected by the collector to the ONU.
- The ONU forwards the power consumption information to an OLT and the OLT forwards the information to the upper-layer device. Then the upper-layer device forwards the information to an AMR server.

Copyright © Huawei Technologies Co., Ltd.

Figure 17-3 Example network for configuring intelligent collection of power consumption information in the electrical power system over Ethernet



NOTE

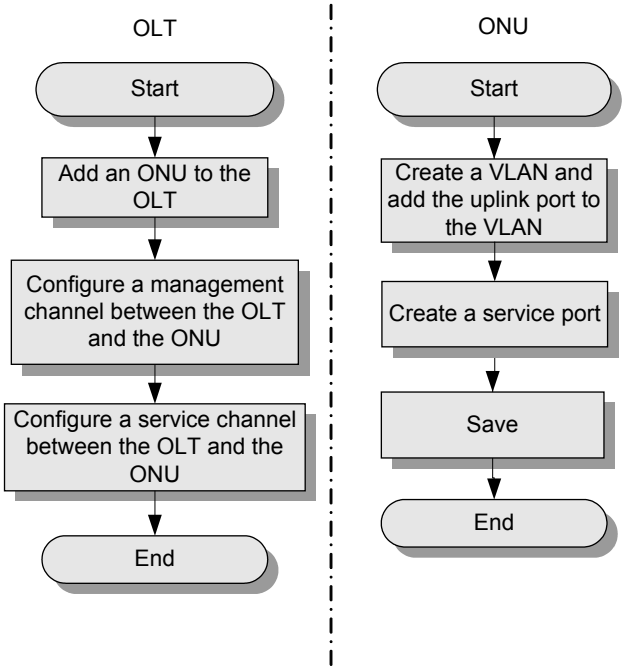
In this example, an MA5621 is used as the ONU.

Configuration Flowchart

Figure 17-4 provides the procedure for configuring intelligent collection of power consumption information in the electrical power system over Ethernet

Copyright © Huawei Technologies Co., Ltd.

Figure 17-4 Procedure for configuring intelligent collection of power consumption information in the electrical power system over Ethernet



Device	Step	Remarks
OLT	1. Add an ONU on an OLT.	You can configure data for an ONU only after it has been added on an OLT.
	2. Configure a management channel between the OLT and the ONU.	After configuring an inband management channel between the OLT and the ONU, you can log in to the ONU on the OLT and configure data for the ONU.
	3. Configure a service channel between the OLT and the ONU.	The power consumption information collected by the ONU is transparently transmitted by the OLT through the upper-layer network to the AMR server.
ONU	1. Create a virtual local area network (VLAN) and add the uplink port to the VLAN.	To transmit packets with a VLAN tag through an uplink port, add the uplink port to the VLAN.
	2. Create a service port.	Create a service port on the ONU to receive the power consumption information. The data is transmitted upstream to the OLT through an uplink port.

Copyright © Huawei Technologies Co., Ltd.

Data Plan

Table 17-3 provides the OLT data plan, and Table 17-4 provides the ONU data plan.

Table 17-3 Data plan for configuring intelligent collection of power consumption information in the electrical power system over Ethernet-OLT side

Item	Data
VLAN	● Uplink port: 0/19/0 ● Inband management VLAN: smart VLAN 8 ● Service VLAN: smart VLAN 100
Inband management IP address	IP address: 192.168.50.20/24
GPON service board	● Port: 0/3/1 ● ONU ID: 1 ● ONU authentication mode: SN ● ONU SN: 48575443E6D8B541
DBA profile	● Profile name: Data ● Type: type3 ● Assured bandwidth: 20 Mbit/s ● Maximum bandwidth: 50 Mbit/s
ONU line profile	● Profile ID: 10, bound to DBA profile Data ● GEM port ID: 0 (used for transmitting inband management service stream) ● GEM port ID: 1 (used for transparently transmitting meter data) ● T-CONT ID: 5
ONU management mode	SNMP

Table 17-4 Data plan for configuring intelligent collection of power consumption information in the electrical power system over Ethernet-ONU side

Configuration Item	Data	Remarks
Inband management IP address	IP address: 192.168.50.2/24	-
Traffic profile	Index 6 (default)	-
Service port	0/1/0	-

Copyright © Huawei Technologies Co., Ltd.

Configuration Item	Data	Remarks
Uplink port	0/0/0	-
Uplink VLAN	smart VLAN 100	The uplink VLAN must be the same as the user VLAN on the OLT.
User VLAN	untagged	-

Procedure

Step 1 Configure the OLT.

1. Create an SVLAN and add an upstream port to it.

   Create smart VLAN 100, and then add upstream port 0/19/0 to the VLAN.

   ```
   huawei(config)#vlan 100 smart
   huawei(config)#port vlan 100 0/19 0
   ```

2. (Optional) Configure upstream link aggregation.

   In this example, a single uplink port is used. In the case of multiple uplink ports, upstream link aggregation can be configured.

3. Configure GPON ONU profiles.

   GPON ONU profiles include the DBA profile, line profile, service profile, and alarm profile.

   - DBA profile: A DBA profile describes the GPON traffic parameters. A T-CONT is bound to a DBA profile for dynamic bandwidth allocation, improving the upstream bandwidth usage rate.
   - Line profile: A line profile describes the binding between the T-CONT and the DBA profile, the QoS mode of the traffic stream, and the mapping between the GEM port and the ONU-side service.
   - Service profile: A service profile provides the service configuration channel for the ONU that is managed through OMCI.
   - Alarm profile: An alarm profile contains a series of alarm thresholds to measure and monitor the performance of activated ONU lines. When a statistical value reaches the threshold, the host is notified and an alarm is reported to the log host and the NMS.

   a. Add a DBA profile.

      You can at first run the **display dba-profile** command to query the DBA profiles existing in the system. If the DBA profiles existing in the system do not meet the requirements, you need to run the **dba-profile add** command to add a DBA profile.

      Configure the profile name to Data, profile type to Type3, assured bandwidth to 20 Mbit/s, and maximum bandwidth to 50 Mbit/s.

      ```
      huawei(config)#dba-profile add profile-name Data type3 assure 20480 max
      51200
      ```


Copyright © Huawei Technologies Co., Ltd.

b. Add an ONU line profile.

Add GPON ONU line profile 10 and bind T-CONT 5 to the DBA profile named Data. In this way, the T-CONT can provide flexible DBA solutions based on different configurations in the DBA profile.

```
huawei(config)#ont-lineprofile gpon profile-id 10
huawei(config-gpon-lineprofile-10)#tcont 5 dba-profile-name Data
```

Add GEM port 0 for transmitting management traffic streams, GEM port 1 for transmitting data traffic streams. Bind GEM port 0 and GEM port 1 to T-CONT 5. Configure the QoS mode to priority-queue (default) and the queue priority to 3.

```
huawei(config-gpon-lineprofile-10)#gem add 0 eth tcont 5 priority-queue 3
huawei(config-gpon-lineprofile-10)#gem add 1 eth tcont 5 priority-queue 3
```

Configure the mapping mode from the GEM port to ONU-side service to VLAN (default), map the service port of management VLAN 8 to GEM port 0, map the service port of SVLAN 100 to GEM port 1.

```
huawei(config-gpon-lineprofile-10)#mapping-mode vlan
huawei(config-gpon-lineprofile-10)#gem mapping 0 0 vlan 8
huawei(config-gpon-lineprofile-10)#gem mapping 1 1 vlan 100
```

After the configuration is complete, run the **commit** command to make the configured parameters take effect.

```
huawei(config-gpon-lineprofile-10)#commit
huawei(config-gpon-lineprofile-10)#quit
```

c. (Optional) Add an alarm profile.

- The ID of the default GPON alarm profile is 1. The thresholds of all the alarm parameters in the default alarm profile are 0, which indicates that no alarm is generated.
- In this example, the default alarm profile is used, and therefore the configuration of the alarm profile is not required.
- Run the **gpon alarm-profile add** command to add an alarm profile, which is used for monitoring the performance of an activated ONU line.

4. Add an ONU on the OLT.

The ONU is connected to the GPON port of the OLT through an optical fiber. You can perform the service configuration only after adding an ONU successfully on the OLT.

a. Add an ONU.

Connect the ONU to GPON port 0/3/1. The ONU ID is 1, the SN is 48575443E6D8B541, the management mode is SNMP, and the bound line profile ID is 10.

There are two ways to add an ONU. Select either of the two ways according to actual conditions.

- Add an ONU offline: If the password or SN of an ONU is obtained, you can run the **ont add** command to add the ONU offline.
- Automatically find an ONU: If the password or SN of an ONU is unknown, run the port ont-auto-find command in the GPON mode to enable the ONU auto-find function of the GPON port. Then, run the **ont confirm** command to confirm the ONU.

To add an ONU offline, do as follows:

```
huawei(config)#interface gpon 0/3
huawei(config-if-gpon-0/3)#ont add 1 1 sn-auth 48575443E6D8B541 snmp ont-
```


Copyright © Huawei Technologies Co., Ltd.

```
lineprofile-id
 10 desc MA5621_0/3/1/1_lineprofile10
```

To automatically find an ONU, do as follows:

```
huawei(config)#interface gpon 0/3
huawei(config-if-gpon-0/3)#port 1 ont-auto-find enable
huawei(config-if-gpon-0/3)#display ont autofind 1
   //After this command is executed, the information about all ONUs
connected to
  //the GPON port through the optical splitter is displayed.

   ------------------------------------------------------------
   Number              : 1
   F/S/P               : 0/3/1
   Ont SN              : 48575443E6D8B541
   Password            :
   VenderID            : HWTC
   Ont Version         : MA5621
   Ont SoftwareVersion : V800R310C00
   Ont EquipmentID     : SmartAX MA5621
   Ont autofind time   : 2011-09-10 11:20:16
   ------------------------------------------------------------
huawei(config-if-gpon-0/3)#ont confirm 1 ontid 1 sn-auth 48575443E6D8B541
snmp ont-lineprofile-id
 10 desc MA5621_0/3/1/1_lineprofile10
```

NOTE

If multiple ONUs of the same type are connected to a port and the same line profile or service profile is bound to the ONUs, you can add ONUs in batches by confirming the auto-found ONUs in batches to simplify the operation and increase the configuration efficiency. For example, the preceding command can be modified as follows:

huawei(config-if-gpon-0/3)#**ont confirm 1 all sn-auth snmp ont-lineprofile-id 10 desc MA5621_0/3/1_lineprofile10**

5. Confirm that the ONU goes online normally.

   After an ONU is added, run the **display ont info** command to query the current status of the ONU. Ensure that **Control flag** of the ONU is **active**, **Run State** is **online**, and **Config state** is **normal**.

```
huawei(config-if-gpon-0/3)#display ont info 1 1

------------------------------------------------------------------------
  F/S/P                :
0/3/1
  ONT-ID               :
1
  Control flag         : active    //Indicates that the ONU is
activated.
  Run state           : online    //Indicates that the ONU already goes online
normally.
  Config state         : normal    //Indicates that the configuration status
of the ONU is normal.
...//The rest of the response information is omitted.

huawei(config-if-gpon-0/3)#quit
```

   If the ONU state fails, the ONU fails to be in the up state, or the ONU does not match, check the ONU state by referring to the above-mentioned descriptions.

   - If **Control flag** is **deactive**, run the **ont activate** command in the GPON port mode to activate the ONU.

Copyright © Huawei Technologies Co., Ltd.

- If the ONU fails to be in the up state, that is, **Run state** is **offline**, the physical line may be broken or the optical transceiver may be damaged. You need to check both the material and the line.
- If the ONU state fails, that is, **Config state** is **failed**, the ONU capability set outmatches the actual ONU capabilities. In this case, run the **display ont failed-configuration** command in the diagnosis mode to check the failed configuration item and the failure cause. Then, rectify the fault according to actual conditions.

  NOTE

  If an ONT supports only four queues, the values of 4-7 of the priority-queue parameter in the gem add command are invalid. After configuration recovers, Config state will be failed.

6. Configure the management channel from the OLT to the ONU.

   NOTE

   Only when the OLT remotely manages the ONU through SNMP, the management channel needs to be configured. When the OLT remotely manages the ONU through OMCI, the management channel need not be configured.

   a. Configure the inband management VLAN and IP address of the OLT.

      To remote log in to the ONU and configure the ONU from the OLT, you must configure the inband management VLANs and IP addresses of the OLT and the ONU on the OLT.

      Create management VLAN 8, and configure the inband management IP address to 192.168.50.20/24.

      ```
      huawei(config)#vlan 8 smart
      huawei(config)#port vlan 8 0/19 0
      huawei(config)#interface vlanif 8
      huawei(config-if-vlanif8)#ip address 192.168.50.20 24
      huawei(config-if-vlanif8)#quit
      ```

   b. Configure the inband management VLAN and IP address of the ONU.

      Configure the static IP address of the ONU to 192.168.50.2/24 and the management VLAN ID to 8 (the same as the management VLAN of the OLT).

      ```
      huawei(config)#interface gpon 0/3
      huawei(config-if-gpon-0/3)#ont ipconfig 1 1 ip-address 192.168.50.2 mask
      255.255.255.0 manage-vlan 8
      ```

   c. Configure an inband management service port.

      Configure the management service port ID to 0, management VLAN ID to 8, GEM port ID to 0, and CVLAN ID to 8. The rate of the inband service port on the OLT is not limited. Therefore, use traffic profile 6 (default). To limit the rate of the service port, run the **traffic table ip** command to add a traffic profile and bind it to the service port.

      ```
      huawei(config)#service-port 0 vlan 8 gpon 0/3/1 ont 1 gemport 0 multi-
      service
      user-vlan 8 rx-cttr 6 tx-cttr 6
      ```

7. Confirm that the management channel between the OLT and the ONU is available.
   - On the OLT, run the **ping *192.168.50.2*** command to check the connectivity to the ONU. The ICMP ECHO-REPLY packet from the ONU should be received.
   - You can remote log in to the ONU from the OLT to perform the configuration.
8. Create a service port.

   Configure the Data service port ID to 1, SVLAN ID to 100, GEM port ID to 1, CVLAN ID to 100. Rate limitation for upstream and downstream packets is performed on the ONU

Copyright © Huawei Technologies Co., Ltd.

instead of on the OLT. Therefore, use traffic profile 6 (default). To limit the rate of the service port, run the **traffic table ip** command to add a traffic profile and bind it to the service port.

The CVLAN must be the same as the upstream VLAN of the ONU.

```
huawei(config)#service-port 1 vlan 100 gpon 0/3/1 ont 1 gemport 1 multi-service
user-vlan 100 rx-cttr 6 tx-cttr 6
```

9. Configure queue scheduling.

   Use the 3PQ+5WRR queue scheduling. Queues 0-4 adopt the WRR mode, with the weights of 10, 10, 20, 20, and 40 respectively; queues 5-7 adopt the PQ mode.

   Queue scheduling is a global configuration. You need to configure queue scheduling only once on the OLT, and then the configuration takes effect globally. In the subsequent phases, you need not configure queue scheduling repeatedly when configuring other services.

   ```
   huawei(config)#queue-scheduler wrr 10 10 20 20 40 0 0 0
   ```

   Configure the mapping between queues and 802.1p priorities. Priorities 0-7 map queues 0-7 respectively.

   For the service board that supports only four queues, the mapping between 802.1p priorities and queue IDs is as follows: priorities 0 and 1 map queue 1; priorities 2 and 3 map queue 2; priorities 4 and 5 map queue 3; priorities 6 and 7 map queue 4.

   ```
   huawei(config)#cos-queue-map cos0 0 cos1 1 cos2 2 cos3 3 cos4 4 cos5 5 cos6 6 cos7 7
   ```

10. Save the data.

    ```
    huawei(config)#save
    ```

Step 2 Configure the ONU.

NOTE

Because the management VLAN and the management IP address have been configured, you can remote log in to the ONU from the OLT to perform the configuration.

1. Log in to the ONU to perform the configuration.

   On the OLT, you can remote log in to the ONU to perform the configuration. User name: **root** (default). Password: **mduadmin** (default).

2. Create a VLAN.

   ```
   huawei(config)#vlan 100 smart
   ```

3. Add an uplink port to the VLAN.

   Add uplink port 0/0/0 to the VLAN.

   ```
   huawei(config)#port vlan 100 0/0 0
   ```

4. Create a service port.

   Create service port 2. Its user VLAN ID is untagged and service VLAN ID is 100. Use the default traffic profile (traffic profile 6). To limit the traffic rate, run the **traffic table ip** command to configure the traffic profile.

   ```
   huawei(config)#service-port 2 vlan 100 eth 0/1/1 multi-service user-vlan
   untagged rx-cttr 6
   tx-cttr 6
   ```


Copyright © Huawei Technologies Co., Ltd.

5. Save the data.
   ```
   huawei(config)#save
   ```

----End

Result

After the preceding configurations are complete, the power consumption information collected by the smart meter is transmitted to the AMR server.

Configuration File

Configure the OLT.

```
vlan 100 smart
port vlan 100 0/19 0
vlan 8 smart
port vlan 8 0/19 0
interface vlanif 8
ip address 192.168.50.20 24
quit
dba-profile add profile-name Data type3 assure 20480 max 51200
ont-lineprofile gpon profile-id 10
tcont 5 dba-profile-name Data
gem add 0 eth tcont 5 priority-queue 3
gem add 1 eth tcont 5 priority-queue 3
mapping-mode vlan
gem mapping 0 0 vlan 8
gem mapping 1 1 vlan 100
commit
quit
interface gpon 0/3
port 1 ont-auto-find enable
ont confirm 1 ontid 1 sn-auth 48575443E6D8B541 snmp ont-lineprofile-id
 10 desc MA5621_0/3/1/1_lineprofile10
ont ipconfig 1 1 static ip-address 192.168.50.2 mask 255.255.255.0 vlan 8
ont alarm-profile 1 1 profile-id 1
service-port 0 vlan 8 gpon 0/3/1 ont 1 gemport 0 multi-service
user-vlan 8 rx-cttr 6 tx-cttr 6
service-port 1 vlan 100 gpon 0/3/1 ont 1 gemport 1 multi-service
user-vlan 100 rx-cttr 6 tx-cttr 6
queue-scheduler wrr 10 10 20 20 40 0 0 0
cos-queue-map cos0 0 cos1 1 cos2 2 cos3 3 cos4 4 cos5 5 cos6 6 cos7 7
save
```

Configure the ONU.

```
vlan 100 smart
port vlan 100 0/0 0
service-port 2 vlan 100 eth 0/1/0 multi-service user-vlan untagged rx-cttr 6 tx-
cttr 6
save
```

17.1.3 Configuration Example of Automatically Transmitting Site Information over Ethernet (Single Homing)

An optical network unit (ONU) can receive site information in the electrical power system through gigabit Ethernet (GE) or fast Ethernet (FE) autonegotiation electrical ports, and automatically transmit the information to an optical line terminal (OLT). The ONU cooperates with an OLT to provide GPON type C single-homing protection, ensuring service reliability. GPON is the acronym for gigabit-capable passive optical network.

Copyright © Huawei Technologies Co., Ltd.

Context

Generic object oriented substation event (GOOSE) is a mechanism defined in IEC 61850 for rapidly transmitting events in a substation automation system. GOOSE packets are multicast packets for communication between terminal units.

In the GPON type C single-homing protection mechanism, the two PON lines between an ONU and an OLT work in active/standby mode and cannot forward packets at the same time.

- If the OLT detects that the upstream link to the active PON port is faulty, the OLT automatically switches services to the upstream link to the standby PON port. In addition, the OLT sends a PON section trace (PST) message to the ONU to notify the ONU of the switching and switching cause over the uplink to the standby PON port, and instructs the ONU to perform the switching.
- If the ONU detects that the downstream link to the active PON port is faulty, the ONU automatically switches services to the downstream link to the standby PON port. In addition, the ONU sends a PST message to the OLT to notify the OLT of the switching and switching cause over the downlink to the standby PON port, and instructs the OLT to perform the switching.

For details about the GPON type C protection mechanism, see *GPON Type C Protection* in *Feature Description*.

Service Requirements

- In a smart grid, terminal units collect the running status information, as well as monitoring and control information about the power distribution system and send the information to the master station system.
- The information collected by terminal units is transparently transmitted to the master station system, and therefore the transmission network must be secure enough to ensure reliable running of the smart grid.
- Terminal units must communicate with each other. This is because, when a breaker is disconnected or the switch position of an isolator switch changes, a terminal unit must directly send the change information to the measuring and monitoring device and the substation monitoring system in real time. GOOSE can rapidly transmit events in a substation automation system, and requires that ONUs connecting to the same or different PON ports support Layer 2 interconnection.
- A terminal unit provides Ethernet access so an ONU can receive the collected information over Ethernet.
- The information is transmitted over a GPON network.

Networking

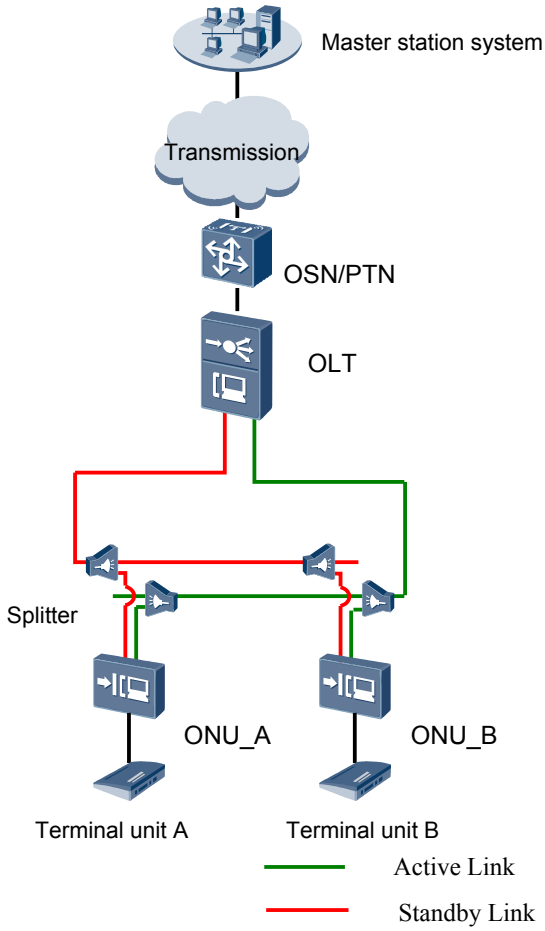
Figure 17-5 shows an example network for configuring automatic transmission of site information in the electrical power system over Ethernet, and the active and standby line connections between the terminal units and the master station system. This example describes how to configure the transmission for terminal unit A connected to ONU_A. The configuration procedure for ONU_B is similar to that for ONU_A.

- ONU_A and ONU_B are connected to terminal units through a GE or FE autonegotiation electrical port. After receiving messages from a terminal unit, ONU_A and ONU_B report the messages to the OLT. The OLT forwards the messages to the master station system.

Copyright © Huawei Technologies Co., Ltd.

- In a single homing scenario, an ONU is connected to one OLT. The OLT provides two passive optical network (PON) ports. An ONU provides two PON ports for upstream transmission, and the backbone fiber, optical splitter, and distribution fiber are configured for redundancy backup. In this scenario, PON type C single-homing protection can be configured to ensure service reliability.

Figure 17-5 Example network for configuring automatic transmission of site information in the electrical power system over Ethernet



NOTE

In this example, an MA5621 is used as the ONU.

Data Plan

Table 17-5 provides the OLT data plan, and Table 17-6 provides the ONU data plan.

Copyright © Huawei Technologies Co., Ltd.

Table 17-5 Data plan for configuring automatic transmission of site information in the electrical power system over Ethernet-OLT side

Device	Item	Data
OLT	Uplink port	Ethernet port: 0/19/0
	VLAN	● Inband management virtual local area network (VLAN): smart VLAN 8 ● Customer VLAN (CVLAN): smart VLAN 200; service VLAN (SVLAN): smart VLAN 200 (used for transmitting the site information about the electrical power system) ● CVLAN: smart VLAN 100; SVLAN: smart VLAN 100 (used for transmitting GOOSE packets)
	Inband management IP address	IP address: 192.168.50.20/24
	GPON service board The GPON service board can be the H801GPBC, H802GPBD, or H805GPBD board.	● Port: – 0/3/1: GPON port connecting to the active line – 0/4/1: GPON port connecting to the standby line ● ONU ID: 1 ● ONU authentication mode: SN ● ONU SN: 48575443E6D8B541
	DBA profile	● Profile name: Data ● Type: type3 ● Assured bandwidth: 20 Mbit/s ● Maximum bandwidth: 50 Mbit/s
	ONU line profile	● Profile ID: 10, bound to the DBA profile named Data ● GEM port ID: 0 (used for transmitting inband management service stream) ● GEM port ID: 1 (used for transparently transmitting the information about the electrical power system) ● GEM port ID: 2 (used for transparently transmitting GOOSE packets) ● T-CONT ID: 5
	ONU management mode	SNMP

Copyright © Huawei Technologies Co., Ltd.

Device	Item	Data
	Priority	The 802.1p priority is used: The priority of the site information about the electrical power system is 1 and the priority of GOOSE packets is 5.

Table 17-6 Data plan for configuring automatic transmission of site information in the electrical power system over Ethernet-ONU side

Device	Configuration Item	Data	Remarks
ONU_A	Inband management IP address	192.168.50.2/24	-
	Traffic profile	● Index 10 (used for transmitting the power distribution site information) ● Index 11 (used for transmitting GOOSE packets)	-
	Service port	Ethernet port: 0/1/1	Port 0/1/1 is used for services on terminal unit A.
	Uplink port	GPON port ● 0/0/0: active uplink port ● 0/0/1: standby uplink port	-
	Uplink VLAN	● Smart VLAN 8 (used for inband management VLAN) ● Smart VLAN 200 (used for transmitting power distribution site information) ● Smart VLAN 100 (used for transmitting GOOSE packets)	The uplink VLAN must be the same as the CVLAN on the OLT.
	Priority	The 802.1p priority is used: The priority of power distribution site information is 1 and the priority of GOOSE packets is 5.	-

Copyright © Huawei Technologies Co., Ltd.

Device	Configuration Item	Data	Remarks
	User-side VLAN	● Untagged (used for transmitting power distribution site information) ● Smart VLAN 2 (used for transmitting GOOSE packets)	-
ONU_B	The data plan is the same as that of ONU_A except for the IP address.		

NOTE

When deploying GPON type C protection, ensure that static MAC address, static Address Resolution Protocol (APR), and Ethernet operation, administration, and maintenance (OAM) functions are not configured on an uplink port. Otherwise, service protection switchover may be affected.

When deploying GPON type C protection, ensure that the configurations of port virtual local area network (VLAN), traffic suppression, line rate, and access control list (ACL) on the two uplink ports on an ONU are the same.

Procedure

Step 1 Configure the OLT.

1. Create an SVLAN and add an uplink port to it.

   Create service VLANs 100 and 200, and then add uplink port 0/19/0 to VLAN 200.

   ```
   huawei(config)#vlan 100,200 smart
   huawei(config)#port vlan 200 0/19 0
   ```

2. (Optional) Configure upstream link aggregation.

   In this example, a single uplink port is used. In the case of multiple uplink ports, upstream link aggregation can be configured.

3. Configure GPON ONU profiles.

   GPON ONU profiles include the DBA profile, line profile, service profile, and alarm profile.

   - DBA profile: A DBA profile describes the GPON traffic parameters. A T-CONT is bound to a DBA profile for dynamic bandwidth allocation, improving the upstream bandwidth usage rate.
   - Line profile: A line profile describes the binding between the T-CONT and the DBA profile, the QoS mode of the traffic stream, and the mapping between the GEM port and the ONU-side service.
   - Service profile: A service profile provides the service configuration channel for the ONU that is managed through OMCI. You do not need to configure a service profile in this configuration example.
   - Alarm profile: An alarm profile contains a series of alarm thresholds to measure and monitor the performance of activated ONU lines. When a statistical value reaches the threshold, the host is notified and an alarm is reported to the log host and the NMS.

Copyright © Huawei Technologies Co., Ltd.

a. Add a DBA profile.

   You can at first run the **display dba-profile** command to query the DBA profiles existing in the system. If the DBA profiles existing in the system do not meet the requirements, you need to run the **dba-profile add** command to add a DBA profile.

   Configure the profile name to Data, profile type to Type3, assured bandwidth to 20 Mbit/s, and maximum bandwidth to 50 Mbit/s.

   ```
   huawei(config)#dba-profile add profile-name Data type3 assure 20480 max
   51200
   ```

b. Add an ONU line profile.

   Add GPON ONU line profile 10 and bind T-CONT 5 to the DBA profile named Data. In this way, the T-CONT can provide flexible DBA solutions based on different configurations in the DBA profile.

   ```
   huawei(config)#ont-lineprofile gpon profile-id 10
   huawei(config-gpon-lineprofile-10)#tcont 5 dba-profile-name Data
   ```

   Add GEM port 0 for transmitting management traffic streams, GEM port 1 for transmitting the electric system site information traffic streams and GEM port 2 for transmitting goose packets traffic streams. Bind GEM port 0, GEM port 1 and GEM port 2 to T-CONT 5. Configure the QoS mode to priority-queue (default) and the queue priority to 3.

   NOTE

   The MA5621 does not support QoS mode **gem-car** or **flow-car**.

   ```
   huawei(config-gpon-lineprofile-10)#gem add 0 eth tcont 5 priority-queue 3
   huawei(config-gpon-lineprofile-10)#gem add 1 eth tcont 5 priority-queue 3
   huawei(config-gpon-lineprofile-10)#gem add 2 eth tcont 5 priority-queue 3
   ```

   Configure the mapping mode from the GEM port to ONU-side service to VLAN (default), map the service port of management VLAN 8 to GEM port 0, map the service port of the site information SVLAN 200 to GEM port 1 and map the service port of the goose packets SVLAN 300 to GEM port 2.

   ```
   huawei(config-gpon-lineprofile-10)#mapping-mode vlan
   huawei(config-gpon-lineprofile-10)#gem mapping 0 0 vlan 8
   huawei(config-gpon-lineprofile-10)#gem mapping 1 1 vlan 200
   huawei(config-gpon-lineprofile-10)#gem mapping 2 2 vlan 300
   ```

   After the configuration is complete, run the **commit** command to make the configured parameters take effect.

   ```
   huawei(config-gpon-lineprofile-10)#commit
   huawei(config-gpon-lineprofile-10)#quit
   ```

c. (Optional) Add an alarm profile.

   - The ID of the default GPON alarm profile is 1. The thresholds of all the alarm parameters in the default alarm profile are 0, which indicates that no alarm is generated.
   - In this example, the default alarm profile is used, and therefore the configuration of the alarm profile is not required.
   - Run the **gpon alarm-profile add** command to add an alarm profile, which is used for monitoring the performance of an activated ONU line.

4. Add an ONU on the OLT.

   The ONU is connected to the GPON port of the OLT through an optical fiber. You can perform the service configuration only after adding an ONU successfully on the OLT.

Copyright © Huawei Technologies Co., Ltd.

a. Add an ONU.

Connect the ONU to GPON port 0/3/1. The ONU ID is 1, the SN is 48575443E6D8B541, the management mode is SNMP, and the bound line profile ID is 10.

There are two ways to add an ONU. Select either of the two ways according to actual conditions.

- Add an ONU offline: If the password or SN of an ONU is obtained, you can run the **ont add** command to add the ONU offline.
- Automatically find an ONU: If the password or SN of an ONU is unknown, run the port **ont-auto-find** command in the GPON mode to enable the ONU auto-find function of the GPON port. Then, run the **ont confirm** command to confirm the ONU.

To add an ONU offline, do as follows:

```
huawei(config)#interface gpon 0/3
huawei(config-if-gpon-0/3)#ont add 1 1 sn-auth 48575443E6D8B541 snmp ont-
lineprofile-id
 10 desc MA5621_0/3/1/1_lineprofile10
```

To automatically find an ONU, do as follows:

```
huawei(config)#interface gpon 0/3
huawei(config-if-gpon-0/3)#port 1 ont-auto-find enable
huawei(config-if-gpon-0/3)#display ont autofind 1
   //After this command is executed, the information about all ONUs
connected to the GPON port through the optical splitter is displayed.

   ------------------------------------------------------------
   Number              : 1
   F/S/P               : 0/3/1
   Ont SN              : 48575443E6D8B541
   Password            :
   VenderID            : HWTC
   Ont Version         : MA5621
   Ont SoftwareVersion : V800R312C00
   Ont EquipmentID     : SmartAX MA5621
   Ont autofind time   : 2012-09-10 11:20:16
   ------------------------------------------------------------
huawei(config-if-gpon-0/3)#ont confirm 1 ontid 1 sn-auth 48575443E6D8B541
snmp ont-lineprofile-id
 10 desc MA5621_0/3/1/1_lineprofile10
```

NOTE

If multiple ONUs of the same type are connected to a port and the same line profile or service profile is bound to the ONUs, you can add ONUs in batches by confirming the auto-found ONUs in batches to simplify the operation and increase the configuration efficiency. For example, the preceding command can be modified as follows: huawei(config-if-gpon-0/3)#**ont confirm 1 all sn-auth snmp ont-lineprofile-id 10 desc MA5621_0/3/1_lineprofile10**.

5. Confirm that the ONU goes online normally.

After an ONU is added, run the **display ont info** command to query the current status of the ONU. Ensure that **Control flag** of the ONU is **active**, **Run State** is **online**, and **Config state** is **normal**.

```
huawei(config-if-gpon-0/3)#display ont info 1 1

------------------------------------------------------------------------
  F/S/P               :
0/3/1
  ONT-ID              :
1
```


Copyright © Huawei Technologies Co., Ltd.

```
  Control flag         : active    //Indicates that the ONU is
activated.
  Run state           : online    //Indicates that the ONU already goes online
normally.
  Config state         : normal    //Indicates that the configuration status
of the ONU is normal.
...//The rest of the response information is omitted.
```

If the ONU state fails, the ONU fails to be in the up state, or the ONU does not match, check the ONU state by referring to the above-mentioned descriptions.

- If **Control flag** is **deactive**, run the **ont activate** command in the GPON port mode to activate the ONU.
- If the ONU fails to be in the up state, that is, **Run state** is **offline**, the physical line may be broken or the optical transceiver may be damaged. You need to check both the material and the line.
- If the ONU state fails, that is, **Config state** is **failed**, the ONU capability set outmatches the actual ONU capabilities. In this case, run the **display ont failed-configuration** command in the diagnosis mode to check the failed configuration item and the failure cause. Then, rectify the fault according to actual conditions.

  NOTE

  If an ONT supports only four queues, the values of 4-7 of the priority-queue parameter in the gem add command are invalid. After configuration recovers, Config state will be failed.

6. Configure the management channel from the OLT to the ONU.

   NOTE

   Only when the OLT remotely manages the ONU through SNMP, the management channel needs to be configured. When the OLT remotely manages the ONU through OMCI, the management channel need not be configured.

   a. Configure the inband management VLAN and IP address of the OLT.

      To log in to the ONU through Telnet and configure the ONU from the OLT, you must configure the inband management VLANs and IP addresses of the OLT and the ONU on the OLT.

      Create management VLAN 8, and configure the inband management IP address to 192.168.50.20/24.

      ```
      huawei(config-if-gpon-0/3)#quit
      huawei(config)#vlan 8 smart
      huawei(config)#port vlan 8 0/19 0
      huawei(config)#interface vlanif 8
      huawei(config-if-vlanif8)#ip address 192.168.50.20 24
      huawei(config-if-vlanif8)#quit
      ```

   b. Configure the inband management VLAN and IP address of the ONU.

      Configure the static IP address of the ONU to 192.168.50.2/24 and the management VLAN ID to 8 (the same as the management VLAN of the OLT).

      ```
      huawei(config)#interface gpon 0/3
      huawei(config-if-gpon-0/3)#ont ipconfig 1 1 ip-address 192.168.50.2 mask
      255.255.255.0 manage-vlan 8
      ```

   c. Configure an inband management service port.

      Configure the management service port ID to 0, management VLAN ID to 8, GEM port ID to 0, and customer VLAN (CVLAN) ID to 8. The rate of the inband service port on the OLT is not limited. Therefore, use traffic profile 6 (default). To limit the rate of the service port, run the **traffic table ip** command to add a traffic profile and bind it to the service port.

Copyright © Huawei Technologies Co., Ltd.

```
huawei(config)#service-port 0 vlan 8 gpon 0/3/1 ont 1 gemport 0 multi-
service
user-vlan 8 rx-cttr 6 tx-cttr 6
```

7. Confirm that the management channel between the OLT and the ONU is available.
   - On the OLT, run the **ping *192.168.50.2*** command to check the connectivity to the ONU. The ICMP ECHO-REPLY packet from the ONU should be received.
   - You can run the **telnet *192.168.50.2*** command to telnet to the ONU and then configure the ONU.
8. Configure a GPON type C protection group.

   Configure cross-board backup on ports 0/3/1 and 0/4/1 on different GPON service boards on the OLT. After the configuration, when port 0/3/1 is faulty, the OLT automatically switches services to port 0/4/1, ensuring services running.

```
huawei(config)#interface gpon 0/4
huawei(config-if-gpon-0/4)#ont add 1 protect-side      //Set the link to port
0/4/1 as the standby link.
huawei(config-if-gpon-0/4)#quit
huawei(config)#protect-group 0 protect-target gpon-uni-ont workmode portstate
huawei(protect-group-0)#protect-group member port 0/3/1 ont 1 role work
huawei(protect-group-0)#protect-group member port 0/4/1 ont 1 role protect
huawei(protect-group-0)#protect-group enable
huawei(protect-group-0)#quit
```

9. Create a service port.

   Configure the site information service port ID to 1, SVLAN ID to 200, CVLAN ID to 200, and GEM port ID to 1, and configure the GOOSE packets service port ID to 2, SVLAN ID to 100, CVLAN ID to 100, and GEM port ID to 2. Rate limitation for upstream and downstream packets is performed on the ONU instead of on the OLT.

   The same port is used for transmitting the site information about the electrical power system and GOOSE packets. Therefore, the 802.1p priority of each service needs to be set. The priority of the site information about the electrical power system is lower than that of GOOSE packets. Set the traffic profile index of the site information about the electrical power system to 20 and the priority to 1; set the traffic profile index of GOOSE packets to 21 and the priority to 5.

   The CVLAN must be the same as the upstream VLAN of the ONU.

```
huawei(config)#traffic table ip index 20 cir off priority 1 priority-policy
local-Setting
  Create traffic descriptor record
successfully

-------------------------------------------------
  TD Index             :
20
  TD Name              : ip-traffic-
table_20
  Priority             :
1
  Copy Priority        :
-
  Mapping Index        :
-
  CTAG Mapping Priority:
-
  CTAG Mapping Index   :
-
  CTAG Default Priority:
0
```


Copyright © Huawei Technologies Co., Ltd.

```
  Priority Policy      : local-
pri
  CIR                  :
off
  CBS                  :
off
  PIR                  :
off
  PBS                  :
off
  Referenced Status    : not
used
  ------------------------------------------------
huawei(config)#traffic table ip index 21 cir off priority 5 priority-policy
local-Setting
  Create traffic descriptor record
successfully

------------------------------------------------
  TD Index             :
21
  TD Name              : ip-traffic-
table_21
  Priority             :
5
  Copy Priority        :
-
  Mapping Index        :
-
  CTAG Mapping Priority:
-
  CTAG Mapping Index   :
-
  CTAG Default Priority:
0
  Priority Policy      : local-
pri
  CIR                  :
off
  CBS                  :
off
  PIR                  :
off
  PBS                  :
off
  Referenced Status    : not
used
  ------------------------------------------------
huawei(config)#service-port 1 vlan 200 gpon 0/3/1 ont 1 gem port 1 multi-
service
user-vlan 200 inbound traffic-table index 20 outbound traffic-table index 20
huawei(config)#service-port 2 vlan 100 gpon 0/3/1 ont 1 gem port 2 multi-
service
user-vlan 100 inbound traffic-table index 21 outbound traffic-table index 21
```

10. Configure the bridging function for GOOSE packets.

    a. Disable the unknown multicast suppression function.

       Goose packets are unknown multicast packets. Disable the unknown multicast suppression function on the OLT to ensure that GOOSE packets are not lost.

       ```
       huawei(config)#multicast-unknown policy service-port 2 transparent
       huawei(config)#vlan service-profile profile-id 20
       huawei(config-vlan-srvprof-20)#packet-policy multicast forward
         Info: Please use the commit command to make modifications take
       effect
       ```


Copyright © Huawei Technologies Co., Ltd.

```
huawei(config-vlan-srvprof-20)#commit
```

b. Enable the bridging function.

To support the electrical GOOSE function, ONU_A must communicate with ONU_B at Layer 2.

```
huawei(config-vlan-srvprof-20)#user-bridging
enable
  Info: Please use the commit command to make modifications take
effect

huawei(config-vlan-srvprof-20)#commit
huawei(config-vlan-srvprof-20)#quit
```

c. Bind the VLAN service profile to the uplink VLAN.

```
huawei(config)#display vlan service-profile profile-id 20


Command:
          display vlan service-profile profile-id
20

  Profile   ID:
20
  Profile Name:
srvprof-20

--------------------------------------------------------------------------

  Parameter                       Committed          Not
Committed

--------------------------------------------------------------------------

  Forwarding mode                 NotConfig
-
  Anti-macspoofing                NotConfig
-
  Anti-ipspoofing                 enable
-
  PPPoE MAC mode                  NotConfig
-
  BPDU tunnel                     NotConfig
-
  RIP tunnel                      NotConfig
-
  VTP-CDP tunnel                  NotConfig
-
  DHCP mode                       n/a
-
  DHCP proxy                      enable
-
  DHCP option82                   enable
-
  PITP                            enable
-
  Broadcast packet policy         NotConfig
-
  Multicast packet policy         forward
-
  Unknown unicast packet policy   NotConfig
-
  User-bridging                   enable
-
  IPoE VMAC                       NotConfig          -
  PPPoE VMAC                      NotConfig          -
  PPPoA VMAC                      NotConfig          -
```


Copyright © Huawei Technologies Co., Ltd.

```
  Mismatch IGMP packet policy      discard
-
  VMAC aging mode                  MAC-learning
-
  OSPF tunnel                      enable
-
  Layer-3 protocol tunnel          enable
-
  Mac-address learning fabric      enable
-
  DHCPv6 mode                      n/a               -
  DHCPv6 option                    enable            -
  PPPoA MAC mode                   NotConfig         -
  Anti-IPv6spoofing                enable            -
  IPv6 DAD proxy                   disable           -
  Bind route and ND                disable           -
  NS-reply function                disable           -
  ARP-reply function               disable           -
  DHCP relay-interface relay-agent NotConfig         -
  ---------------------------------------------------------------------------
  Binding VLAN list            : 0
  ---------------------------------------------------------------------------
huawei(config)#vlan bind service-profile 100 profile-id 20
```

11. Configure queue scheduling.

    The GOOSE service traffic is forwarded in PQ mode.

    Queue scheduling is a global configuration. You need to configure queue scheduling only once on the OLT, and then the configuration takes effect globally. In the subsequent phases, you need not configure queue scheduling repeatedly when configuring other services.

    ```
    huawei(config)#queue-scheduler strict-priority
    ```

    Configure the mapping between queues and 802.1p priorities. Priorities 0-7 map queues 0-7 respectively.

    For the service board that supports only four queues, the mapping between 802.1p priorities and queue IDs is as follows: priorities 0 and 1 map queue 1; priorities 2 and 3 map queue 2; priorities 4 and 5 map queue 3; priorities 6 and 7 map queue 4.

    ```
    huawei(config)#cos-queue-map cos0 0 cos1 1 cos2 2 cos3 3 cos4 4 cos5 5 cos6 6
    cos7 7
    ```

12. Save the data.

    ```
    huawei(config)#save
    ```

Step 2 The following describes the procedure for configuring the automatic transmission of site information about the electrical power system over Ethernet on ONU_A.

NOTE

Because the management VLAN and the management IP address have been configured, you can run the **telnet** ***192.168.50.2*** command on the OLT to log in to the ONU to perform the configuration. You can also log in to the ONU through a serial port to perform the configuration.

1. Log in to the ONU to perform the configuration.

   On the OLT, use the management IP address of the ONU to log in to the ONU through Telnet. User name: **root** (default). Password: **mduadmin** (default).

   ```
   huawei(config)#telnet 192.168.50.2
   { <cr>|service-port<U><0,4294967295> }:

     Command:
             telnet 192.168.50.2
     Press CTRL_] to quit telnet mode
   ```


Copyright © Huawei Technologies Co., Ltd.

```
  Trying 192.168.50.2 ...
  Connected to 192.168.50.2 ...
>>User name:root
>>User password:      //It is not displayed on the console.
```

2. Configure the dual PON ports upstream mode.

   For GPON type C single-homing protection, set the dual PON ports upstream mode to **Active-standby uplink mode**.

```
huawei(config)#pon uplink-mode active-standby
```

3. Configure a traffic profile.

   The same port is used for transmitting power distribution site information and GOOSE packets. Therefore, the 802.1p priority of each service needs to be set. The priority of power distribution site information is lower than that of GOOSE packets. Set the traffic profile index of power distribution site information to 10 and the priority to 1; set the traffic profile index of GOOSE packets to 11 and the priority to 5.

```
huawei(config)#traffic table ip index 10 cir off priority 1 priority-policy
local-Setting
  Create traffic descriptor record
successfully

-------------------------------------------------
  TD Index             :
10
  TD Name              : ip-traffic-
table_10
  Priority             :
1
  Copy Priority        :
-
  CTAG Mapping Priority:
-
  CTAG Default Priority:
0
  Priority Policy      : local-
pri
  CIR                  :
off
  CBS                  :
off
  PIR                  :
off
  PBS                  :
off
  Color Mode           : color-
blind
  Referenced Status    : not
used
  -------------------------------------------------
huawei(config)#traffic table ip index 11 cir off priority 5 priority-policy
local-Setting
  Create traffic descriptor record
successfully

-------------------------------------------------
  TD Index             :
11
  TD Name              : ip-traffic-
table_11
  Priority             :
5
  Copy Priority        :
-
```


Copyright © Huawei Technologies Co., Ltd.

```
  CTAG Mapping Priority:
-
  CTAG Default Priority:
0
  Priority Policy      : local-
pri
  CIR                  :
off
  CBS                  :
off
  PIR                  :
off
  PBS                  :
off
  Color Mode           : color-
blind
  Referenced Status    : not
used
  ------------------------------------------------
```

4. Create VLANs.

```
huawei(config)#vlan 100,200 smart           //Create SVLANs for service
transmission from ONU_A to the OLT
```

5. Add an uplink port to the VLANs.

   Add uplink port 0/0/0 and 0/0/1 to the VLANs.

```
huawei(config)#port vlan 100,200 0/0 0-1
```

6. Create service ports.

   For power distribution site information, create service port 2 with SVLAN 200 and traffic profile 10.

```
huawei(config)#service-port 2 vlan 200 eth 0/1/1 multi-service user-vlan
untagged
 rx-cttr 10 tx-cttr 10
```

   For GOOSE packets, create service port 3 with SVLAN 100, CVLAN 2 and traffic profile 11.

```
huawei(config)#service-port 3 vlan 100 eth 0/1/1 multi-service user-vlan 2 rx-
cttr 11 tx-cttr 11
```

7. Configure the bridging function for GOOSE packets.

   a. Disable the unknown multicast suppression function.

      Goose packets are unknown multicast packets. Disable the unknown multicast suppression function on the OLT to ensure that GOOSE packets are not lost.

```
huawei(config)#vlan service-profile profile-id 10
huawei(config-vlan-srvprof-10)#packet-policy multicast forward
  Info: Please use the commit command to make modifications take
effect

huawei(config-vlan-srvprof-10)#commit
```

   b. Enable the bridging function.

```
huawei(config-vlan-srvprof-10)#user-bridging
enable
  Info: Please use the commit command to make modifications take
effect

huawei(config-vlan-srvprof-10)#commit
huawei(config-vlan-srvprof-10)#quit
```

   c. Bind the VLAN service profile to the uplink VLAN.

Copyright © Huawei Technologies Co., Ltd.

```
huawei(config)#display vlan service-profile profile-id 10


Command:
          display vlan service-profile profile-id
10

  Profile   ID:
10
  Profile Name:
srvprof-10

------------------------------------------------------------------------

  Parameter                         Committed          Not
Committed

------------------------------------------------------------------------

  Forwarding mode                   VLAN-MAC
-
  BPDU tunnel                       disable
-
  RIP tunnel                        disable
-
  VTP-CDP tunnel                    disable
-
  Multicast packet policy           forward
-
  User-bridging                     enable
-
  OSPF tunnel                       enable
-

------------------------------------------------------------------------

  Binding VLAN list            :
0

------------------------------------------------------------------------
huawei(config)#vlan bind service-profile 100 profile-id 10
```

d. In ETH mode, disable the unknown multicast suppression function on the user interface and uplink port.

```
huawei(config)#interface eth 0/1
huawei(config-if-eth-0/1)#undo traffic-suppress 1 multicast
huawei(config-if-eth-0/1)#quit
huawei(config)#interface eth 0/0
huawei(config-if-eth-0/0)#undo traffic-suppress all multicast
huawei(config-if-eth-0/0)#quit
```

8. Set the queue scheduling mode to strict priority queue (PQ).

   The GOOSE service traffic is forwarded in PQ mode.

```
huawei(config)#queue-scheduler strict-priority
```

9. Save the data.

```
huawei(config)#save
```

----End

Result

After the master station server queries the power distribution site information, the power distribution site information is transmitted to the master station server.

Copyright © Huawei Technologies Co., Ltd.

Configuration File

Configure OLT_A.

```
vlan 100,200 smart
port vlan 200 0/19 0
dba-profile add profile-name Data type3 assure 20480 max 51200
ont-lineprofile gpon profile-id 10
tcont 5 dba-profile-name Data
gem add 0 eth tcont 5 priority-queue 3
gem add 1 eth tcont 5 priority-queue 3
gem add 2 eth tcont 5 priority-queue 3
mapping-mode vlan
gem mapping 0 0 vlan 8
gem mapping 1 1 vlan 200
gem mapping 2 2 vlan 100
commit
quit
interface gpon 0/3
port 1 ont-auto-find enable
ont confirm 1 ontid 1 sn-auth 48575443E6D8B541 snmp ont-lineprofile-id
 10 desc MA5621_0/3/1/1_lineprofile10
quit
vlan 8 smart
port vlan 8 0/19 0
interface vlanif 8
ip address 192.168.50.20 24
quit
interface gpon 0/3
ont ipconfig 1 1 ip-address 192.168.50.2 mask 255.255.255.0 manage-vlan 8
service-port 0 vlan 8 gpon 0/3/1 ont 1 gemport 0 multi-service
user-vlan 8 rx-cttr 6 tx-cttr 6
interface gpon 0/4
ont add 1 protect-side
quit
protect-group 0 protect-target gpon-uni-ont workmode portstate
protect-group member port 0/3/1 ont 1 role work
protect-group member port 0/4/1 ont 1 role protect
protect-group enable
quit
traffic table ip index 20 cir off priority 1 priority-policy local-Setting
traffic table ip index 21 cir off priority 5 priority-policy local-Setting
service-port 1 vlan 200 gpon 0/3/1 ont 1 gemport 1 multi-service
user-vlan 200 inbound traffic-table index 20 outbound traffic-table index 20
service-port 2 vlan 100 gpon 0/3/1 ont 1 gemport 2 multi-service
user-vlan 100 gemport 2 inbound traffic-table index 21 outbound traffic-table index
21
multicast-unknown policy service-port 2 transparent
vlan service-profile profile-id 20
packet-policy multicast forward
user-bridging enable
commit
quit
vlan bind service-profile 100 profile-id 20
queue-scheduler strict-priority
cos-queue-map cos0 0 cos1 1 cos2 2 cos3 3 cos4 4 cos5 5 cos6 6 cos7 7
save
```

Configure ONU_A.

```
pon uplink-mode active-standby
traffic table ip index 10 cir off priority 1 priority-policy local-Setting
traffic table ip index 11 cir off priority 5 priority-policy local-Setting
vlan 100,200 smart
port vlan 100,200 0/0 0-1
service-port 2 vlan 200 eth 0/1/1 multi-service user-vlan untagged
 rx-cttr 10 tx-cttr 10
```


Copyright © Huawei Technologies Co., Ltd.

```
service-port 3 vlan 100 eth 0/1/1 multi-service user-vlan 2 rx-cttr 11 tx-cttr 11
packet-policy multicast forward
user-bridging enable
commit
quit
vlan bind service-profile 100 profile-id 10
interface eth 0/1
undo traffic-suppress 1 multicast
quit
interface eth 0/0
undo traffic-suppress all multicast
quit
squeue-scheduler strict-priority
save
```

17.1.4 Configuration Example of Automatically Transmitting Site Information over Ethernet (Dual Homing)

An optical network unit (ONU) can automatically transmit power distribution site information in the electrical power system through gigabit Ethernet (GE) or fast Ethernet (FE) autonegotiation electrical ports. The ONU cooperates with an optical line terminal (OLT) to provide GPON type C dual-homing protection, ensuring service reliability. GPON is the acronym for gigabit-capable passive optical network.

Context

Generic object oriented substation event (GOOSE) is a mechanism defined in IEC 61850 for rapidly transmitting events in a substation automation system. GOOSE packets are multicast packets for communication between terminal units.

On a type C dual-homing GPON network, the two PON links between an OLT and an ONU work in active/standby mode and they cannot forward packets at the same time. When the active link is faulty due to a component fault, the ONU can rapidly switch services to the standby OLT. If a protection group is bound to the status of an upstream Ethernet port or Bidirectional Forwarding Detection (BFD) sessions on an optical line terminal (OLT), namely, a protection group is associated with the status of an upstream Ethernet port of BFD sessions, the OLT notifies the ONU of performing an active/standby switchover to restore services when the OLT upstream network fails to be connected or an OLT Layer 2 physical link fails. For details about the GPON type C protection mechanism, see *GPON Type C Protection* in *Feature Description*.

Service Requirements

- In a smart grid, terminal units collect the running status information, as well as monitoring and control information about the power distribution system and send the information to the master station system.
- The information collected by terminal units is transparently transmitted to the master station system, and therefore the transmission network must be secure enough to ensure reliable running of the smart grid.
- Terminal units must communicate with each other. This is because, when a breaker is disconnected or the switch position of an isolator switch changes, a terminal unit must directly send the change information to the measuring and monitoring device and the substation monitoring system in real time. GOOSE can rapidly transmit events in a substation automation system, and requires that ONUs connecting to the same or different PON ports support Layer 2 interconnection.

Copyright © Huawei Technologies Co., Ltd.

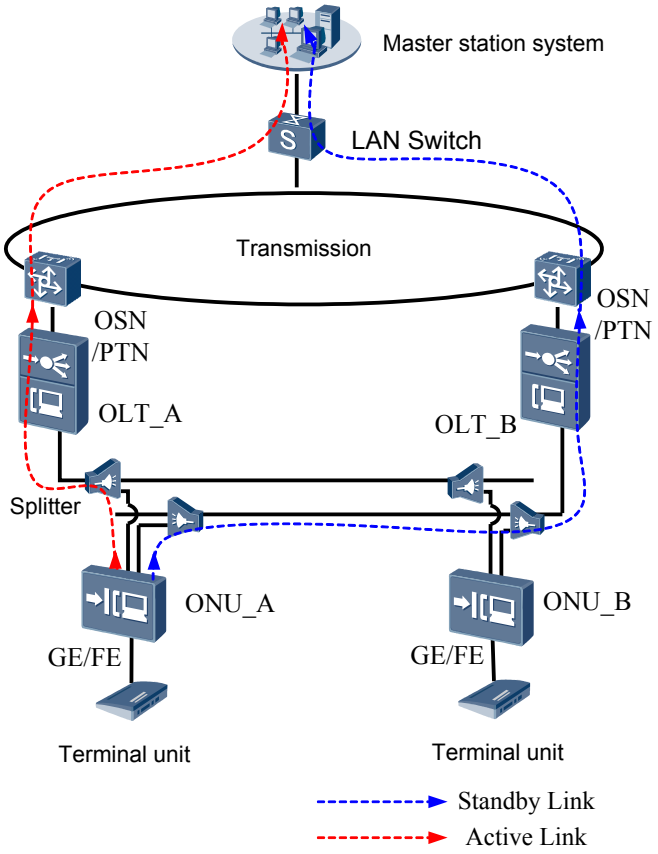
- A terminal unit provides Ethernet access so an ONU can receive the collected information over Ethernet.
- The information is transmitted over a GPON network.

Networking

Figure 17-6 shows an example network for configuring the automatic transmission of power distribution site information in the electrical power system over Ethernet.

- ONU_A and ONU_B are connected to terminal units through a GE or FE autonegotiation electrical port. After receiving messages from a terminal unit, ONU_A and ONU_B report the messages to the OLT. The OLT forwards the messages to the master station system.
- In a dual homing scenario, an ONU is connected to two OLTs. Each OLT provides a passive optical network (PON) port. An ONU provides two PON ports for upstream transmission, and the backbone fiber, optical splitter, and distribution fiber are configured for redundancy backup. In this scenario, GPON type C dual-homing protection can be configured to ensure service reliability.

Figure 17-6 Example network for configuring automatic transmission of power distribution site information in the electrical power system over Ethernet



NOTE

In this example, an MA5621 is used as the ONU.

Copyright © Huawei Technologies Co., Ltd.

Data Plan

Table 17-7 provides the OLT data plan, and Table 17-8 provides the ONU data plan.

Table 17-7 Data plan for configuring automatic transmission of power distribution site information in the electrical power system over Ethernet-OLT side

Device	Item	Data
OLT_A	Uplink port	0/19/0
	VLAN	Inband management VLAN: smart VLAN 8 Service VLAN (SVLAN): smart VLAN 200 (used for transmitting the site information about the electrical power system) SVLAN: smart VLAN 101 (used for transmitting GOOSE packets)
	Inband management IP address	192.168.50.20/24
	GPON service board The GPON service board can be an H801GPBC, H802GPBD, or H805GPBD board.	Port: 0/3/1 ONU ID: 1 ONU authentication mode: SN ONU SN: 48575443E6D8B541
	DBA profile	Profile name: Data Type: type3 Assured bandwidth: 20 Mbit/s Maximum bandwidth: 50 Mbit/s
	ONU line profile	● Profile ID: 10, bound to the DBA profile named Data ● GEM port ID: 0 (used for transmitting inband management service stream) ● GEM port ID: 1 (used for transparently transmitting the information about the electrical power system) ● GEM port ID: 2 (used for transparently transmitting GOOSE packets) ● T-CONT ID: 5
	ONU management mode	SNMP
	Priority	The 802.1p priority is used: The priority of the site information about the electrical power system is 1 and the priority of GOOSE packets is 6.

Copyright © Huawei Technologies Co., Ltd.

Device	Item	Data
	Associated protection switching	A protection group is associated with the status of upstream Ethernet ports. **NOTE** ● To detect the link status at the IP layer (the connection status of the OLT upstream network), you need to associate the protection group with BFD sessions. ● To detect a Layer 2 physical link fault, you need to associate the protection group with the status of the upstream Ethernet port. In this example, the protection group is associated with the status of the upstream Ethernet port.
OLT_B	The data plan is the same as that of OLT_A.	

Table 17-8 Data plan for configuring automatic transmission of power distribution site information in the electrical power system over Ethernet-ONU side

Device	Configuration Item	Data	Remarks
ONU_A	Inband management IP address	IP address: 192.168.50.2/24	-
	Traffic profile	● Index 10 (used for transmitting the power distribution site information) ● Index 11 (used for transmitting GOOSE packets)	-
	Service port	Eth port: 0/1/1	-
	Uplink port	GPON port: 0/0/0, 0/0/1	-
	Uplink VLAN	● Smart VLAN 100 (used for transmitting power distribution site information) ● Smart VLAN 101 (used for transmitting GOOSE packets)	The uplink VLAN must be the same as the CVLAN on the OLT.
	Priority	The 802.1p priority is used: The priority of power distribution site information is 1 and the priority of GOOSE packets is 6.	-

Copyright © Huawei Technologies Co., Ltd.

Device	Configuration Item	Data	Remarks
	User-side VLAN	Untagged (used for transmitting power distribution site information) Smart VLAN 2 (used for transmitting GOOSE packets)	-
ONU_B	The data plan is the same as that of ONU_A except for the IP address.		

NOTE

When deploying GPON type C dual-homing protection, ensure that static MAC address, static Address Resolution Protocol (APR), and Ethernet operation, administration, and maintenance (OAM) functions are not configured on an uplink port. Otherwise, service protection switchover may be affected.

When deploying GPON type C dual-homing protection, ensure that the configurations of port virtual local area network (VLAN), traffic suppression, line rate, and access control list (ACL) on the two uplink ports on an ONU are the same.

Procedure

Step 1 Configure the OLT.

1. Create an SVLAN and add an uplink port to it.

   Create smart VLAN 101 and VLAN 200, and then add uplink port 0/19/0 to these VLANs.

   ```
   huawei(config)#vlan 101,200 smart
   huawei(config)#port vlan 200 0/19 0
   ```

2. (Optional) Configure upstream link aggregation.

   In this example, a single uplink port is used. In the case of multiple uplink ports, upstream link aggregation can be configured.

3. Configure GPON ONU profiles.

   GPON ONU profiles include the DBA profile, line profile, service profile, and alarm profile.

   - DBA profile: A DBA profile describes the GPON traffic parameters. A T-CONT is bound to a DBA profile for dynamic bandwidth allocation, improving the upstream bandwidth usage rate.
   - Line profile: A line profile describes the binding between the T-CONT and the DBA profile, the QoS mode of the traffic stream, and the mapping between the GEM port and the ONU-side service.
   - Service profile: A service profile provides the service configuration channel for the ONU that is managed through OMCI. You do not need to configure a service profile in this configuration example.
   - Alarm profile: An alarm profile contains a series of alarm thresholds to measure and monitor the performance of activated ONU lines. When a statistical value reaches the threshold, the host is notified and an alarm is reported to the log host and the NMS.

   a. Add a DBA profile.

Copyright © Huawei Technologies Co., Ltd.

You can at first run the **display dba-profile** command to query the DBA profiles existing in the system. If the DBA profiles existing in the system do not meet the requirements, you need to run the **dba-profile add** command to add a DBA profile.

Configure the profile name to Data, profile type to Type3, assured bandwidth to 20 Mbit/s, and maximum bandwidth to 50 Mbit/s.

```
huawei(config)#dba-profile add profile-name Data type3 assure 20480 max
51200
```

b. Add an ONU line profile.

Add GPON ONU line profile 10 and bind T-CONT 5 to the DBA profile named Data. In this way, the T-CONT can provide flexible DBA solutions based on different configurations in the DBA profile.

```
huawei(config)#ont-lineprofile gpon profile-id 10
huawei(config-gpon-lineprofile-10)#tcont 5 dba-profile-name Data
```

Add GEM port 0 for transmitting management traffic streams, GEM port 1 for transmitting the electrical power system site information traffic streams and GEM port 2 for transmitting GOOSE packets traffic streams. Bind GEM port 0, GEM port 1 and GEM port 2 to T-CONT 5. Configure the QoS mode to priority-queue (default) and the queue priority to 3.

NOTE

The MA5621 does not support QoS mode **gem-car** or **flow-car**.

```
huawei(config-gpon-lineprofile-10)#gem add 0 eth tcont 5 priority-queue 3
huawei(config-gpon-lineprofile-10)#gem add 1 eth tcont 5 priority-queue 3
huawei(config-gpon-lineprofile-10)#gem add 2 eth tcont 5 priority-queue 3
```

Configure the mapping mode from the GEM port to ONU-side service to VLAN (default), map the service port of management VLAN 8 to GEM port 0, map the service port of the site information SVLAN 200 to GEM port 1 and map the service port of the GOOSE packets SVLAN 101 to GEM port 2.

```
huawei(config-gpon-lineprofile-10)#mapping-mode vlan
huawei(config-gpon-lineprofile-10)#gem mapping 0 0 vlan 8
huawei(config-gpon-lineprofile-10)#gem mapping 1 1 vlan 200
huawei(config-gpon-lineprofile-10)#gem mapping 2 2 vlan 101
```

After the configuration is complete, run the **commit** command to make the configured parameters take effect.

```
huawei(config-gpon-lineprofile-10)#commit
huawei(config-gpon-lineprofile-10)#quit
```

c. (Optional) Add an alarm profile.

- The ID of the default GPON alarm profile is 1. The thresholds of all the alarm parameters in the default alarm profile are 0, which indicates that no alarm is generated.
- In this example, the default alarm profile is used, and therefore the configuration of the alarm profile is not required.
- Run the **gpon alarm-profile add** command to add an alarm profile, which is used for monitoring the performance of an activated ONU line.

4. Add an ONU on the OLT.

The ONU is connected to the GPON port of the OLT through an optical fiber. You can perform the service configuration only after adding an ONU successfully on the OLT.

a. Add an ONU.

Copyright © Huawei Technologies Co., Ltd.

Connect the ONU to GPON port 0/3/1. The ONU ID is 1, the SN is 48575443E6D8B541, the management mode is SNMP, and the bound line profile ID is 10.

There are two ways to add an ONU. Select either of the two ways according to actual conditions.

- Add an ONU offline: If the password or SN of an ONU is obtained, you can run the **ont add** command to add the ONU offline.
- Automatically find an ONU: If the password or SN of an ONU is unknown, run the port **ont-auto-find** command in the GPON mode to enable the ONU auto-find function of the GPON port. Then, run the **ont confirm** command to confirm the ONU.

To add an ONU offline, do as follows:

```
huawei(config)#interface gpon 0/3
huawei(config-if-gpon-0/3)#ont add 1 1 sn-auth 48575443E6D8B541 snmp ont-
lineprofile-id
 10 desc MA5621_0/3/1/1_lineprofile10
```

To automatically find an ONU, do as follows:

```
huawei(config)#interface gpon 0/3
huawei(config-if-gpon-0/3)#port 1 ont-auto-find enable
huawei(config-if-gpon-0/3)#display ont autofind 1
   //After this command is executed, the information about all ONUs
connected to the GPON port through the optical splitter is displayed.

   ------------------------------------------------------------
   Number              : 1
   F/S/P               : 0/3/1
   Ont SN              : 48575443E6D8B541
   Password            :
   VenderID            : HWTC
   Ont Version         : MA5621
   Ont SoftwareVersion : V800R312C00
   Ont EquipmentID     : SmartAX MA5621
   Ont autofind time   : 2012-09-10 11:20:16
   ------------------------------------------------------------
huawei(config-if-gpon-0/3)#ont confirm 1 ontid 1 sn-auth 48575443E6D8B541
snmp ont-lineprofile-id
 10 desc MA5621_0/3/1/1_lineprofile10
```

NOTE

If multiple ONUs of the same type are connected to a port and the same line profile or service profile is bound to the ONUs, you can add ONUs in batches by confirming the auto-found ONUs in batches to simplify the operation and increase the configuration efficiency. For example, the preceding command can be modified as follows: huawei(config-if-gpon-0/3)#**ont confirm 1 all sn-auth snmp ont-lineprofile-id 10 desc MA5621_0/3/1_lineprofile10**.

5. Confirm that the ONU goes online normally.

   After an ONU is added, run the **display ont info** command to query the current status of the ONU. Ensure that **Control flag** of the ONU is **active**, **Run State** is **online**, and **Config state** is **normal**.

```
huawei(config-if-gpon-0/3)#display ont info 1 1

------------------------------------------------------------------------
  F/S/P               :
0/3/1
  ONT-ID              :
1
  Control flag        : active    //Indicates that the ONU is
activated.
```


Copyright © Huawei Technologies Co., Ltd.

```
  Run state           : online    //Indicates that the ONU already goes online
normally.
  Config state         : normal    //Indicates that the configuration status
of the ONU is normal.
...//The rest of the response information is omitted.
```

If the ONU state fails, the ONU fails to be in the up state, or the ONU does not match, check the ONU state by referring to the above-mentioned descriptions.

- If **Control flag** is **deactive**, run the **ont activate** command in the GPON port mode to activate the ONU.
- If the ONU fails to be in the up state, that is, **Run state** is **offline**, the physical line may be broken or the optical transceiver may be damaged. You need to check both the material and the line.
- If the ONU state fails, that is, **Config state** is **failed**, the ONU capability set outmatches the actual ONU capabilities. In this case, run the **display ont failed-configuration** command in the diagnosis mode to check the failed configuration item and the failure cause. Then, rectify the fault according to actual conditions.

  NOTE

  If an ONT supports only four queues, the values of 4-7 of the priority-queue parameter in the gem add command are invalid. After configuration recovers, Config state will be failed.

6. Configure the management channel from the OLT to the ONU.

   NOTE

   Only when the OLT remotely manages the ONU through SNMP, the management channel needs to be configured. When the OLT remotely manages the ONU through OMCI, the management channel need not be configured.

   a. Configure the inband management VLAN and IP address of the OLT.

      To log in to the ONU through Telnet and configure the ONU from the OLT, you must configure the inband management VLANs and IP addresses of the OLT and the ONU on the OLT.

      Create management VLAN 8, and configure the inband management IP address to 192.168.50.20/24.

      ```
      huawei(config-if-gpon-0/3)#quit
      huawei(config)#vlan 8 smart
      huawei(config)#port vlan 8 0/19 0
      huawei(config)#interface vlanif 8
      huawei(config-if-vlanif8)#ip address 192.168.50.20 24
      huawei(config-if-vlanif8)#quit
      ```

   b. Configure the inband management VLAN and IP address of the ONU.

      Configure the static IP address of the ONU to 192.168.50.2/24 and the management VLAN ID to 8 (the same as the management VLAN of the OLT).

      ```
      huawei(config)#interface gpon 0/3
      huawei(config-if-gpon-0/3)#ont ipconfig 1 1 ip-address 192.168.50.2 mask
      255.255.255.0 manage-vlan 8
      ```

   c. Configure an inband management service port.

      Configure the management service port ID to 0, management VLAN ID to 8, GEM port ID to 0, and customer VLAN (CVLAN) ID to 8. The rate of the inband service port on the OLT is not limited. Therefore, use traffic profile 6 (default). To limit the rate of the service port, run the **traffic table ip** command to add a traffic profile and bind it to the service port.

Copyright © Huawei Technologies Co., Ltd.

```
huawei(config)#service-port 0 vlan 8 gpon 0/3/1 ont 1 gemport 0 multi-
service
user-vlan 8 rx-cttr 6 tx-cttr 6
```

7. Confirm that the management channel between the OLT and the ONU is available.
   - On the OLT, run the **ping *192.168.50.2*** command to check the connectivity to the ONU. The ICMP ECHO-REPLY packet from the ONU should be received.
   - You can run the **telnet *192.168.50.2*** command to telnet to the ONU and then configure the ONU.
8. Configure a GPON type C protection group.

   Set OLT_A as the active OLT and OLT_B as the standby OLT. Configure a protection group on both OLT_A and OLT_B. Set the group member status on OLT_A to work and the group member status on OLT_B to protect. After the setting, when the active OLT is faulty, the system automatically switches to the standby OLT, ensuring service running.

   NOTE

   - For a working port, the protect group is enabled by default and you do not need to enable it any more. For a protect port, the protect group is disabled by default. Run the **protect-group enable** command to enable the protect group.
   - Run the **protect-group member port 0/3/1 ont 1 role protect** command on OLT_B to specify the member type in a protect group to protect. Other configurations are the same as that on OLT_A.

```
huawei(config)#protect-group 0 protect-target gpon-uni-ont workmode dual-
parenting
huawei(protect-group-0)#protect-group member port 0/3/1 ont 1 role work
huawei(protect-group-0)#protect-group enable//Determine whether to run this
command based on the type of the member type in a protect group on the port
huawei(protect-group-0)#quit
```

9. Create a service port.

   Configure the site information service port ID to 1, SVLAN ID to 200, GEM port ID to 1, and CVLAN ID to 100, and configure the GOOSE packets service port ID to 2, SVLAN ID to 101, GEM port ID to 2, and CVLAN ID to 101. Rate limitation for upstream and downstream packets is performed on the ONU instead of on the OLT.

   The same port is used for transmitting the site information about the electrical power system and GOOSE packets. Therefore, the 802.1p priority of each service needs to be set. The priority of the site information about the electrical power system is lower than that of GOOSE packets. Set the traffic profile index of the site information about the electrical power system to 20 and the priority to 1; set the traffic profile index of GOOSE packets to 21 and the priority to 6.

   The CVLAN must be the same as the upstream VLAN of the ONU.

```
huawei(config)#traffic table ip index 20 cir off priority 1 priority-policy
local-Setting
  Create traffic descriptor record
successfully

-------------------------------------------------
  TD Index             :
20
  TD Name              : ip-traffic-
table_20
  Priority             :
1
  Copy Priority        :
-
  Mapping Index        :
```


Copyright © Huawei Technologies Co., Ltd.

```
-
  CTAG Mapping Priority:
-
  CTAG Mapping Index   :
-
  CTAG Default Priority:
0
  Priority Policy      : local-
pri
  CIR                  :
off
  CBS                  :
off
  PIR                  :
off
  PBS                  :
off
  Referenced Status    : not
used
  ------------------------------------------------
huawei(config)#traffic table ip index 21 cir off priority 6 priority-policy
local-Setting
  Create traffic descriptor record
successfully

------------------------------------------------
  TD Index             :
21
  TD Name              : ip-traffic-
table_21
  Priority             :
6
  Copy Priority        :
-
  Mapping Index        :
-
  CTAG Mapping Priority:
-
  CTAG Mapping Index   :
-
  CTAG Default Priority:
0
  Priority Policy      : local-
pri
  CIR                  :
off
  CBS                  :
off
  PIR                  :
off
  PBS                  :
off
  Referenced Status    : not
used
  ------------------------------------------------
huawei(config)#service-port 1 vlan 200 gpon 0/3/1 ont 1 gemport 1 multi-
service
user-vlan 100 rx-cttr 20 tx-cttr 20
huawei(config)#service-port 2 vlan 101 gpon 0/3/1 ont 1 gemport 2 multi-
service
user-vlan 101 rx-cttr 21 tx-cttr 21
```

10. Configure the bridging function for GOOSE packets.

    a. Disable the unknown multicast suppression function.

       Goose packets are unknown multicast packets. Disable the unknown multicast suppression function on the OLT to ensure that GOOSE packets are not lost.

Copyright © Huawei Technologies Co., Ltd.

```
huawei(config)#multicast-unknown policy service-port 2 transparent
huawei(config)#vlan service-profile profile-id 20
huawei(config-vlan-srvprof-20)#packet-policy multicast forward
  Info: Please use the commit command to make modifications take
effect

huawei(config-vlan-srvprof-20)#commit
```

b. Enable the bridging function.

To support the electrical GOOSE function, ONU_A must communicate with ONU_B at Layer 2.

```
huawei(config-vlan-srvprof-20)#user-bridging
enable
  Info: Please use the commit command to make modifications take
effect

huawei(config-vlan-srvprof-20)#commit
huawei(config-vlan-srvprof-20)#quit
```

c. Bind the VLAN service profile to the uplink VLAN.

```
huawei(config)#display vlan service-profile profile-id 20


Command:
          display vlan service-profile profile-id
20

  Profile   ID:
20
  Profile Name:
srvprof-20

------------------------------------------------------------------------

  Parameter                         Committed          Not
Committed

------------------------------------------------------------------------

  Forwarding mode                   NotConfig
-
  Anti-macspoofing                  NotConfig
-
  Anti-ipspoofing                   enable
-
  PPPoE MAC mode                    NotConfig
-
  BPDU tunnel                       NotConfig
-
  RIP tunnel                        NotConfig
-
  VTP-CDP tunnel                    NotConfig
-
  DHCP mode                         n/a
-
  DHCP proxy                        enable
-
  DHCP option82                     enable
-
  PITP                              enable
-
  Broadcast packet policy           NotConfig
-
  Multicast packet policy           forward
-
  Unknown unicast packet policy     NotConfig
-
```


Copyright © Huawei Technologies Co., Ltd.

```
  User-bridging                    enable
-
  IPoE VMAC                        NotConfig          -
  PPPoE VMAC                       NotConfig          -
  PPPoA VMAC                       NotConfig          -
  Mismatch IGMP packet policy      discard
-
  VMAC aging mode                  MAC-learning
-
  OSPF tunnel                      enable
-
  Layer-3 protocol tunnel          enable
-
  Mac-address learning fabric      enable
-
  DHCPv6 mode                      n/a                -
  DHCPv6 option                    enable             -
  PPPoA MAC mode                   NotConfig          -
  Anti-IPv6spoofing                enable             -
  IPv6 DAD proxy                   disable            -
  Bind route and ND                disable            -
  NS-reply function                disable            -
  ARP-reply function               disable            -
  DHCP relay-interface relay-agent NotConfig          -
  ---------------------------------------------------------------------------
  Binding VLAN list            : 0
  ---------------------------------------------------------------------------
huawei(config)#vlan bind service-profile 101 profile-id 20
```

11. Configure queue scheduling.

    The GOOSE service traffic is forwarded in PQ mode.

    Queue scheduling is a global configuration. You need to configure queue scheduling only once on the OLT, and then the configuration takes effect globally. In the subsequent phases, you need not configure queue scheduling repeatedly when configuring other services.

    ```
    huawei(config)#queue-scheduler strict-priority
    ```

    Configure the mapping between queues and 802.1p priorities. Priorities 0-7 map queues 0-7 respectively.

    For the service board that supports only four queues, the mapping between 802.1p priorities and queue IDs is as follows: priorities 0 and 1 map queue 1; priorities 2 and 3 map queue 2; priorities 4 and 5 map queue 3; priorities 6 and 7 map queue 4.

    ```
    huawei(config)#cos-queue-map cos0 0 cos1 1 cos2 2 cos3 3 cos4 4 cos5 5 cos6 6
    cos7 7
    ```

12. Associated a protection group with an upstream Ethernet port.

    ```
    huawei(config)#protect-group 0
    huawei(protect-group-0)#uplink-monitor port 0/19/0
    huawei(protect-group-0)#quit
    ```

    NOTE

    If an Ethernet link aggregation group is configured, the Ethernet port that is associated with the dual-homing protection group must be the primary port in the aggregation group. Use the **uplink-monitor bfd** command to associate the protection group with BFD sessions. For the configuration of BFD, please refer to **Configuring the BFD** in **OLT Configuration Guide**.

13. Save the data.

    ```
    huawei(config)#save
    ```

Step 2 The following describes the procedure for configuring the automatic transmission of site information about the electrical power system over Ethernet on ONU_A.

Copyright © Huawei Technologies Co., Ltd.

NOTE

Because the management VLAN and the management IP address have been configured, you can run the **telnet *192.168.50.2*** command on the OLT to log in to the ONU to perform the configuration. You can also log in to the ONU through a serial port to perform the configuration.

1. Log in to the ONU to perform the configuration.

   On the OLT, use the management IP address of the ONU to log in to the ONU through Telnet. User name: **root** (default). Password: **mduadmin** (default).

```
huawei(config)#telnet 192.168.50.2
{ <cr>|service-port<U><0,4294967295> }:

  Command:
          telnet 192.168.50.2
  Press CTRL_] to quit telnet mode
  Trying 192.168.50.2 ...
  Connected to 192.168.50.2 ...
>>User name:root
>>User password:       //It is not displayed on the console.
```

2. Configure the dual PON ports upstream mode.

   When GPON type C dual-homing protect is configured, set the two PON uplink ports to be in the active/standby mode. Run the **display pon config** command to query the working mode of the two ports. The two ports work in active/standby mode by default. Run the **pon uplink-mode active-standby** command to set the mode.

```
huawei(config)#pon uplink-mode active-standby//Determine whether to run this
command based on the dual PON ports upstream mode
```

3. Configure a traffic profile.

   The same port is used for transmitting power distribution site information and GOOSE packets. Therefore, the 802.1p priority of each service needs to be set. The priority of power distribution site information is lower than that of GOOSE packets. Set the traffic profile index of power distribution site information to 10 and the priority to 1; set the traffic profile index of GOOSE packets to 11 and the priority to 6.

```
huawei(config)#traffic table ip index 10 cir off priority 1 priority-policy
local-Setting
  Create traffic descriptor record
successfully

-------------------------------------------------
  TD Index              :
10
  TD Name               : ip-traffic-
table_10
  Priority              :
1
  Copy Priority         :
-
  CTAG Mapping Priority:
-
  CTAG Default Priority:
0
  Priority Policy       : local-
pri
  CIR                   :
off
  CBS                   :
off
  PIR                   :
off
  PBS                   :
```


Copyright © Huawei Technologies Co., Ltd.

```
off
  Color Mode           : color-
blind
  Referenced Status    : not
used
  ------------------------------------------------
huawei(config)#traffic table ip index 11 cir off priority 6 priority-policy
local-Setting
  Create traffic descriptor record
successfully

------------------------------------------------
  TD Index             :
11
  TD Name              : ip-traffic-
table_11
  Priority             :
6
  Copy Priority        :
-
  CTAG Mapping Priority:
-
  CTAG Default Priority:
0
  Priority Policy      : local-
pri
  CIR                  :
off
  CBS                  :
off
  PIR                  :
off
  PBS                  :
off
  Color Mode           : color-
blind
  Referenced Status    : not
used
  ------------------------------------------------
```

4. Create VLANs.

```
huawei(config)#vlan 100 smart
huawei(config)#vlan 101 smart
```

5. Add an uplink port to the VLANs.

   Add uplink port 0/0/0 and 0/0/1 to the VLANs.

```
huawei(config)#port vlan 100 0/0 0-1
huawei(config)#port vlan 101 0/0 0-1
```

6. Create a service port.

   For power distribution site information, create service port 2 with SVLAN 100 and traffic profile 10. For GOOSE packets, create service port 3 with SVLAN 101 and traffic profile 11.

```
huawei(config)#service-port 2 vlan 100 eth 0/1/1 multi-service user-vlan
untagged
 rx-cttr 10 tx-cttr 10
huawei(config)#service-port 3 vlan 101 eth 0/1/1 multi-service user-vlan 2 rx-
cttr 11 tx-cttr 11
```

7. Configure the bridging function for GOOSE packets.

   a. Disable the unknown multicast suppression function.

      Goose packets are unknown multicast packets. Disable the unknown multicast suppression function on the OLT to ensure that GOOSE packets are not lost.

Copyright © Huawei Technologies Co., Ltd.

```
huawei(config)#vlan service-profile profile-id 10
huawei(config-vlan-srvprof-10)#packet-policy multicast forward
  Info: Please use the commit command to make modifications take
effect

huawei(config-vlan-srvprof-10)#commit
```

b. Enable the bridging function.

```
huawei(config-vlan-srvprof-10)#user-bridging
enable
  Info: Please use the commit command to make modifications take
effect

huawei(config-vlan-srvprof-10)#commit
huawei(config-vlan-srvprof-10)#quit
```

c. Bind the VLAN service profile to the uplink VLAN.

```
huawei(config)#display vlan service-profile profile-id 10


Command:
          display vlan service-profile profile-id
10

  Profile   ID:
10
  Profile Name:
srvprof-10

------------------------------------------------------------------------

  Parameter                         Committed          Not
Committed

------------------------------------------------------------------------

  Forwarding mode                   VLAN-MAC
-
  BPDU tunnel                       disable
-
  RIP tunnel                        disable
-
  VTP-CDP tunnel                    disable
-
  Multicast packet policy           forward
-
  User-bridging                     enable
-
  OSPF tunnel                       enable
-

------------------------------------------------------------------------

  Binding VLAN list            :
0

------------------------------------------------------------------------
huawei(config)#vlan bind service-profile 101 profile-id 10
```

d. In ETH mode, disable the unknown multicast suppression function on the user side interface and uplink port.

```
huawei(config)#interface eth 0/1
huawei(config-if-eth-0/1)#undo traffic-suppress 1 multicast
huawei(config-if-eth-0/1)#quit
huawei(config)#interface eth 0/0
huawei(config-if-eth-0/0)#undo traffic-suppress all multicast
huawei(config-if-eth-0/0)#quit
```


Copyright © Huawei Technologies Co., Ltd.

8. Set the queue scheduling mode to strict priority queue (PQ).

   The GOOSE service traffic is forwarded in PQ mode.

   ```
   huawei(config)#queue-scheduler strict-priority
   ```

9. Save the data.

   ```
   huawei(config)#save
   ```

Step 3 The following describes the procedure for configuring the automatic transmission of site information about the electrical power system over Ethernet on ONU_B.

The procedure is the same as that on ONU_A except for the ID of the uplink VLAN used for transmitting power distribution site information and IP address.

----End

Result

After the master station server queries the power distribution site information, the power distribution site information is transmitted to the master station server.

Configuration File

Configure the OLT_A.

```
vlan 101,200 smart
port vlan 200 0/19 0
vlan 8 smart
port vlan 8 0/19 0
interface vlanif 8
ip address 192.168.50.20 24
quit
dba-profile add profile-name Data type3 assure 20480 max 51200
ont-lineprofile gpon profile-id 10
tcont 5 dba-profile-name Data
gem add 0 eth tcont 5 priority-queue 3
gem add 1 eth tcont 5 priority-queue 3
gem add 2 eth tcont 5 priority-queue 3
mapping-mode vlan
gem mapping 0 0 vlan 8
gem mapping 1 1 vlan 200
gem mapping 2 2 vlan 101
commit
quit
interface gpon 0/3
port 1 ont-auto-find enable
ont confirm 1 ontid 1 sn-auth 48575443E6D8B541 snmp ont-lineprofile-id
 10 desc MA5621_0/3/1/1_lineprofile10
ont ipconfig 1 1 static ip-address 192.168.50.2 mask 255.255.255.0 vlan 8
ont alarm-profile 1 1 profile-id 1
service-port 0 vlan 8 gpon 0/3/1 ont 1 gemport 0 multi-service
user-vlan 8 rx-cttr 6 tx-cttr 6
protect-group 0 protect-target gpon-uni-ont workmode dual-parenting
protect-group member port 0/3/1 ont 1 role work
protect-group enable
quit
traffic table ip index 20 cir off priority 1 priority-policy local-Setting
traffic table ip index 21 cir off priority 6 priority-policy local-Setting
service-port 1 vlan 200 gpon 0/3/1 ont 1 gemport 1 multi-service
user-vlan 100 rx-cttr 20 tx-cttr 20
service-port 2 vlan 101 gpon 0/3/1 ont 1 gemport 2 multi-service
multicast-unknown policy service-port 2 transparent
user-vlan 101 rx-cttr 21 tx-cttr 21
```


Copyright © Huawei Technologies Co., Ltd.

```
vlan service-profile profile-id 20
packet-policy multicast forward
user-bridging enable
commit
quit
vlan bind service-profile 101 profile-id 20
queue-scheduler strict-priority
cos-queue-map cos0 0 cos1 1 cos2 2 cos3 3 cos4 4 cos5 5 cos6 6 cos7 7
protect-group 0
uplink-monitor port 0/19/0
quit
save
```

Configure the ONU_A.

```
pon uplink-mode active-standby
traffic table ip index 10 cir off priority 1 priority-policy local-Setting
traffic table ip index 11 cir off priority 6 priority-policy local-Setting
vlan 100 smart
vlan 101 smart
port vlan 100 0/0 0-1
port vlan 101 0/0 0-1
service-port 2 vlan 100 eth 0/1/1 multi-service user-vlan untagged rx-cttr 10 tx-
cttr 10
service-port 3 vlan 101 eth 0/1/1 multi-service user-vlan 2 rx-cttr 11 tx-cttr 11
vlan service-profile profile-id 10
packet-policy multicast forward
user-bridging enable
commit
quit
vlan bind service-profile 101 profile-id 10
interface eth 0/1
undo traffic-suppress 1 multicast
quit
interface eth 0/0
undo traffic-suppress all multicast
quit
squeue-scheduler strict-priority
save
```

17.1.5 Configuration Example of Transmitting Information Collected in Centralized Mode in the Smart Grid over a Serial Port

An optical network unit (ONU) supports the serial port access service, and transmits the service upstream to an optical line terminal (OLT) through a gigabit-capable passive optical network (GPON) port. Then the OLT forwards the service data to upper-layer devices. This process intelligently collects power consumption information in an electrical power system.

Service Requirements

- In an electrical power system, a large amount of meter data needs to be collected in centralized mode in real time and sent to an automatic meter reading system (AMR) server for monitoring and processing.
- A user-side smart meter has a serial port, through which the ONU connects to the smart meter.
- Data is transmitted over a GPON network.

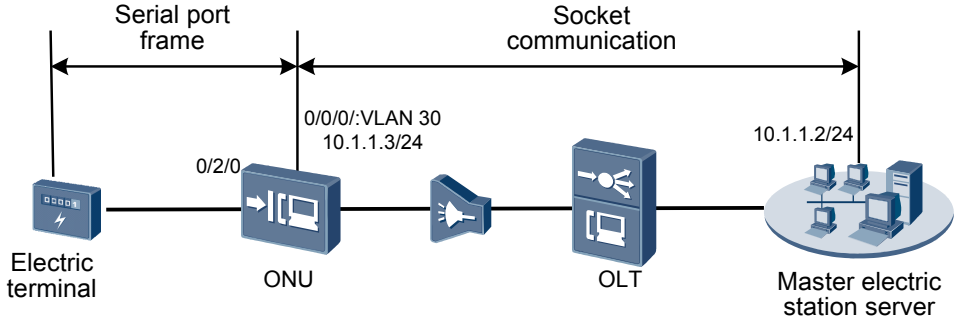
Copyright © Huawei Technologies Co., Ltd.

Networking

Figure 17-7 shows the network diagram for transmitting information collected in centralized mode in the smart grid over a serial port.

- A terminal unit collects meter information and transparently transmits it to an AMR server through an ONU serial port.
- An ONU obtains serial port data through its serial port, encapsulates the serial port data into User Datagram Protocol (UDP) or Transmission Control Protocol (TCP) packets, and transmits the packets upstream to an OLT through a GPON port. The OLT forwards the packets to an upper-layer device and finally to the AMR server. After receiving the UDP or TCP packets sent downstream from the AMR server, the ONU restores the UDP or TCP packets to serial port data flows and transmits the data flows to terminal units.

Figure 17-7 Network diagram for transmitting information collected in centralized mode in the smart grid over a serial port



NOTE

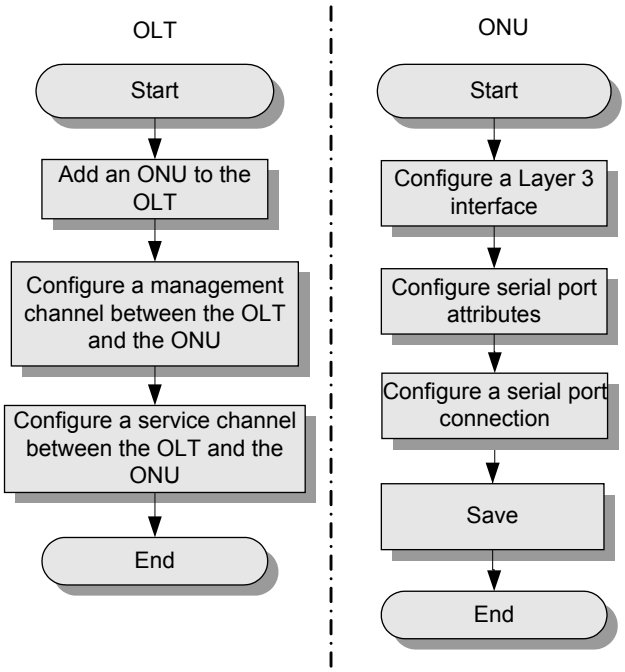
This example uses an MA5621 as an ONU.

Configuration Flowchart

Figure 17-8 shows the flowchart for transmitting information collected in centralized mode in the smart grid over a serial port.

Copyright © Huawei Technologies Co., Ltd.

Figure 17-8 Flowchart for transmitting information collected in centralized mode in the smart grid over a serial port



Device	Configuration Procedure	Configuration Description
OLT	1. Add an ONU to the OLT.	You can configure the ONU only after adding it to the OLT.
	2. Configure a management channel between the OLT and the ONU.	You can log in to the ONU from the OLT and configure the ONU only after the inband management channel between the OLT and the ONU is available.
	3. Configure a service channel between the OLT and the ONU.	The meter data collected by the ONU needs to be transparently transmitted to the AMR server on the upper-layer network through the OLT.
ONU	1. Configure a Layer 3 interface.	The data collected by an ONU needs to carry IP addresses so that it can be transmitted over an IP network.
	2. Configure serial port attributes.	An ONU can communicate with a terminal unit properly only when they have the same serial port attributes.
	3. Configure a serial port connection.	The data collected by an ONU is converted between serial port lines and the Ethernet network through this serial port connection.

Copyright © Huawei Technologies Co., Ltd.

Data Plan

Table 17-9 provides the data plan for the optical line terminal (OLT) and Table 17-10 provides the data plan for the ONU.

Table 17-9 Data plan for the OLT

Configuration Item	Data
Virtual local area network (VLAN)	● Uplink port: 0/19/0 ● Inband management VLAN 8 with VLAN type smart ● Service VLAN 30 with VLAN type smart
IP address	Inband management IP address: 192.168.50.10/24
GPON service board	● Port ID: 0/3/1 ● ONT ID: 1 ● ONU authentication mode: SN ● ONU serial number (SN): 48575443E6D8B541
Dynamic bandwidth allocation (DBA) profile	● Profile name: SerialAccess ● Type: type3 ● Assured bandwidth: 20 Mbit/s ● Maximum bandwidth: 50 Mbit/s
ONU line profile	● ONU line profile 10 bound to DBA profile **SerialAccess** ● GPON encapsulation mode (GEM) port ID: 0 (inband management service port ID) ● GEM port ID: 1 (transparent transmission service port ID) ● Transmission container (T-CONT) ID: 5
ONU management mode	Simple Network Management Protocol (SNMP)

Table 17-10 Data plan for the ONU

Configuration Item	Data	Remarks
Attributes of the inband management interface	● Uplink port: 0/0/0 ● VLAN ID: 8 ● Inband management IP address: 192.168.50.2/24 ● Index of a traffic profile: 6 (default value)	-

Copyright © Huawei Technologies Co., Ltd.

Configuration Item	Data	Remarks
Attributes of the VLAN Layer 3 interface	● Uplink port: 0/0/0 ● VLAN ID: 30 ● IP address of the VLAN Layer 3 interface: 10.1.1.3	The IP address of the master station server is 10.1.1.2.
Attributes of the serial port	● Serial port ID: 0/2/0 ● Working mode: rs485 ● Baud rate: 2400 bit/s	The default baud rate specified in the DL645-2007 Multi-Function Watt-Hour Meter Communication Protocol is 2400 bit/s. Ensure that the serial port attributes are the same as those on the interconnected terminal unit.
Connections of the serial port	● Connection ID: 1 ● Transmission mode: tcp-server ● Local port ID: 3000 ● Serial port frame type: none	If a remote port ID is not specified on an ONU, the system obtains the port ID based on the connection packets received on the serial port from the remote port. **NOTE** When specifying a remote port ID on an ONU, ensure that it is the same as the ID of the source port sending connection packets.

Procedure

Step 1 Configure the OLT.

1. Create a service VLAN and add an uplink port to it.

   The ID of the service VLAN is 30 and the uplink port added to service VLAN 30 is 0/19/0.

   ```
   huawei(config)#vlan 30 smart
   huawei(config)#port vlan 30 0/19 0
   ```

2. (Optional) Configure uplink aggregation.

Copyright © Huawei Technologies Co., Ltd.

This topic uses a single uplink port as an example. If there are multiple uplink ports, configure uplink aggregation.

3. Configure GPON ONU profiles.

   GPON ONU profiles include the DBA profile, line profile, service profile, and alarm profile.

   - DBA profile: describes GPON traffic parameters. A T-CONT is bound to a DBA profile to allocate dynamic bandwidths, improving upstream bandwidth usage.
   - Line profile: describes the binding between T-CONTs and DBA profiles, quality of service (QoS) mode of a service port, and mapping between GEM ports and ONU services.
   - Service profile: provides service configuration channels for an ONU that is managed through an optical network terminal management and control interface (OMCI).
   - Alarm profile: contains a series of alarm thresholds to measure and monitor the performance of activated ONT lines. When a statistical value reaches the threshold, a PON board on the OLT notifies the OLT of this event and sends an alarm to a log host and the network management system (NMS).

   a. Configure a DBA profile.

      Run the **display dba-profile** command to query existing DBA profiles in the system. If the existing DBA profiles in the system cannot meet site requirements, run the **dba-profile add** command to add a DBA profile.

      Set the DBA profile parameters as follows: profile name **SerialAccess**, type Type3, assured bandwidth 20 Mbit/s, and maximum bandwidth 50 Mbit/s.

      ```
      huawei(config)#dba-profile add profile-name SerialAccess type3 assure
      20480 max 51200
      ```

   b. Configure an ONU line profile.

      Add GPON ONU line profile 10 and bind T-CONT 5 to DBA profile **SerialAccess**. Then the T-CONT can provide flexible DBA solutions based on different DBA profile configurations.

      ```
      huawei(config)#ont-lineprofile gpon profile-id 10
      huawei(config-gpon-lineprofile-10)#tcont 5 dba-profile-name SerialAccess
      ```

      Add GEM port 0 to carry management service streams and GEM port 1 to carry service flows for collecting information in the smart grid. Bind GEM ports 0 and 1 to T-CONT 5. Set the QoS mode to priority-queue (default mode) and the queue priority to 3.

      ```
      huawei(config-gpon-lineprofile-10)#gem add 0 eth tcont 5 priority-queue 3
      huawei(config-gpon-lineprofile-10)#gem add 1 eth tcont 5 priority-queue 3
      ```

   Configure the mapping mode between GEM ports and ONU services to VLAN (default mode), map service flows of management VLAN 8 to GEM port 0, and map service flows of service VLAN 30 to GEM port 1.

   ```
   huawei(config-gpon-lineprofile-10)#mapping-mode vlan
   huawei(config-gpon-lineprofile-10)#gem mapping 0 0 vlan 8
   huawei(config-gpon-lineprofile-10)#gem mapping 1 1 vlan 30
   ```

   After the configuration is complete, run the **commit** command to make the configuration take effect.

   ```
   huawei(config-gpon-lineprofile-10)#commit
   huawei(config-gpon-lineprofile-10)#quit
   ```

   (Optional) Configure an alarm profile.

Copyright © Huawei Technologies Co., Ltd.

- The default alarm profile is GPON alarm profile 1, in which each alarm threshold is 0, indicating that no alarm is reported.
- This topic uses the default alarm profile. Therefore, you do not need to configure the profile.
- If necessary, run the **gpon alarm-profile add** command to add a GPON alarm profile to measure and monitor the performance of activated ONT lines.

4. Add an ONU to the OLT.

   The ONU connects to a GPON port on the OLT using an optical fiber. You can configure services only after adding the ONU to the OLT.

   a. Add the ONU.

      Connect the ONU to GPON port 0/3/1 using an optical splitter. The ONU ID is 1, the SN is 48575443E6D8B541, the management mode is SNMP, and the ID of the bound line profile is 10.

      You can use either of the following methods to add an ONU:

      - Add an ONU in offline mode. If you have obtained the password or SN of an ONU, run the **ont add** command to add it in offline mode.
      - Use the ONU automatic discovery function. If the password or SN of an ONU is unknown, run the **port ont-auto-find** command in GPON mode to enable the ONU automatic discovery function. Then run the **ont confirm** command to confirm the automatically discovered ONU.

      To add an ONU in offline mode, run the following commands:

```
huawei(config)#interface gpon 0/3
huawei(config-if-gpon-0/3)#ont add 1 1 sn-auth 48575443E6D8B541 snmp ont-
lineprofile-id
 10 desc MA5621_0/3/1/1_lineprofile10
```

      To add an ONU using the ONU automatic discovery function, run the following commands:

```
huawei(config)#interface gpon 0/3
huawei(config-if-gpon-0/3)#port 1 ont-auto-find enable
huawei(config-if-gpon-0/3)#display ont autofind 1
   //This command displays the information about all ONUs connected to the
GPON port using an optical splitter.

   ------------------------------------------------------------
   Number              : 1
   F/S/P               : 0/3/1
   Ont SN              : 48575443E6D8B541
   Password            :
   VenderID            : HWTC
   Ont Version         : MA5621
   Ont SoftwareVersion : V800R310C00
   Ont EquipmentID     : SmartAX MA5621
   Ont autofind time   : 2011-09-10 11:20:16
   ------------------------------------------------------------
huawei(config-if-gpon-0/3)#ont confirm 1 ontid 1 sn-auth 48575443E6D8B541
snmp ont-lineprofile-id
 10 desc MA5621_0/3/1/1_lineprofile10
```


Copyright © Huawei Technologies Co., Ltd.

NOTE

If a port on the OLT connects to multiple ONUs of the same type and the port on the OLT is bound to the same line profile or service profile, you can add ONUs in batches by confirming the automatically discovered ONUs in batches. This function simplifies operations and improves configuration efficiency. For example, in the preceding information, huawei(config-if-gpon-0/3)#**ont confirm 1 ontid 1 sn-auth 48575443E6D8B541 snmp ont-lineprofile-id 10 desc MA5621_0/3/1/1_lineprofile10** can be changed to huawei(config-if-gpon-0/3)#**ont confirm 1 all sn-auth snmp ont-lineprofile-id 10 desc MA5621_0/3/1_lineprofile10**.

5. Confirm that the ONU goes online properly.

   After adding the ONU, run the **display ont info** command to query the ONU status. Ensure that **Control flag** is **active**, **Run State** is **online**, and **Config state** is **normal**.

```
huawei(config-if-gpon-0/3)#display ont info 1 1

------------------------------------------------------------------------
  F/S/P                   :
0/3/1
  ONT-ID                  :
1
  Control flag            : active    //The ONU has been
activated.
  Run state               : online    //The ONU is
online.
  Config state            : normal    //The ONU configuration status has been
restored.
...//The follow-up terminal display is omitted.
```

   If the ONU status is abnormal, the ONU cannot be in the up state, or the ONU does not meet requirements, check the ONU status based on the preceding information.

   - If **Control flag** is **deactive**, run the **ont activate** command in GPON port mode to activate the ONU.
   - If the ONU cannot be in the up state (**Run state** is **offline**), check materials and lines because the physical line may be cut or the optical module may be damaged.
   - If the ONU status is abnormal (**Config state** is **failed**), ONU capabilities cannot support the configured ONU capability set. Then run the **display ont failed-configuration** command in diagnosis mode to check failed configuration items and failure causes. Then, rectify the fault based on site requirements.

     NOTE

     If an ONT supports only four queues, the values 4 through 7 of the **priority-queue** parameter in the **gem add** command are invalid, which causes **Config state** to be **failed**.

6. Configure a management channel from the OLT to the ONU.

   NOTE

   A management channel needs to be configured only when the OLT remotely manages the ONU using SNMP.

   a. Configure the inband management VLAN for the OLT and set the inband management IP address.

      To log in to the ONU from the OLT and configure the ONU remotely, configure the inband management VLAN for the OLT and the ONU and set the inband management IP address.

      Configure inband management VLAN 8 and set the inband management IP address to 192.168.50.10/24.

```
huawei(config-if-gpon-0/3)#quit
huawei(config)#vlan 8 smart
```


Copyright © Huawei Technologies Co., Ltd.

```
huawei(config)#port vlan 8 0/19 0
huawei(config)#interface vlanif 8
huawei(config-if-vlanif8)#ip address 192.168.50.10 24
huawei(config-if-vlanif8)#quit
```

b. Configure the inband management VLAN for the ONU and set the inband management IP address.

   Set the static IP address of the ONU to 192.168.50.2/24 and management VLAN 8 (the same as the management VLAN for the OLT).

```
huawei(config)#interface gpon 0/3
huawei(config-if-gpon-0/3)#ont ipconfig 1 1 ip-address 192.168.50.2 mask
255.255.255.0 manage-vlan 8
```

c. Configure an inband management service port.

   Configure the management service port ID to 0, management VLAN ID to 8, GEM port ID to 0, and customer VLAN ID to 8. The rate of the inband service port on the OLT is not limited. Therefore, use traffic profile 6 (default profile). To limit the rate of the service port, run the **traffic table ip** command to add a traffic profile and bind it to the service port.

```
huawei(config)#service-port 0 vlan 8 gpon 0/3/1 ont 1 gemport 0 multi-
service
user-vlan 8 rx-cttr 6 tx-cttr 6
```

7. Verify that the management channel between the OLT and the ONU is available.
   - Run the **ping** ***192.168.50.2*** command on the OLT to check the connectivity to the ONU. If the OLT can receive ICMP ECHO-REPLY packets sent from the ONU, the OLT is connected to the ONU.
   - Run the **telnet** ***192.168.50.2*** command to log in to the ONU and configure it.
8. Create a service port.

   Configure the ID of the service port for the power distribution site information to 1, service VLAN ID to 30, and customer VLAN ID to 30. In addition, the traffic of upstream and downstream packets is not limited.

   Ensure that the customer VLAN is the same as the Layer 3 interface VLAN of the ONU.

```
huawei(config)#traffic table ip index 20 cir off priority 1 priority-policy
local-Setting
  Create traffic descriptor record
successfully

-------------------------------------------------
  TD Index             :
20
  TD Name              : ip-traffic-
table_20
  Priority             :
1
  Copy Priority        :
-
  Mapping Index        :
-
  CTAG Mapping Priority:
-
  CTAG Mapping Index   :
-
  CTAG Default Priority:
0
  Priority Policy      : local-
pri
  CIR                  :
```


Copyright © Huawei Technologies Co., Ltd.

```
off
  CBS                  :
off
  PIR                  :
off
  PBS                  :
off
  Referenced Status    : not
used
  ----------------------------------------------
huawei(config)#service-port 1 vlan 30 gpon 0/3/1 ont 1 gemport 1 multi-
service
user-vlan 30 rx-cttr 20 tx-cttr 20
```

9. Configure queue scheduling.

   Use the 3PQ+5WRR queue scheduling. PQ is the acronym for priority queuing and WRR is the acronym for weighted round robin. Queues 0-4 use the WRR mode, with the weights of 10, 10, 20, 20, and 40 respectively. Queues 5-7 use the PQ mode.

   Queue scheduling is a global configuration. Specifically, you need to configure queue scheduling only once on the OLT. Then the configuration takes effect globally. In follow-up operations, you do not need to configure queue scheduling repeatedly when configuring other services.

   ```
   huawei(config)#queue-scheduler wrr 10 10 20 20 40 0 0 0
   ```

   Configure the mapping between queues and 802.1p priorities. Priorities 0-7 map queues 0-7.

   If a board supports only four queues, the mapping between 802.1p priorities and queue IDs is as follows: Priorities 0 and 1 map queue 1. Priorities 2 and 3 map queue 2. Priorities 4 and 5 map queue 3. Priorities 6 and 7 map queue 4.

   ```
   huawei(config)#cos-queue-map cos0 0 cos1 1 cos2 2 cos3 3 cos4 4 cos5 5 cos6 6
   cos7 7
   ```

10. Save the data.

    ```
    huawei(config)#save
    ```

Step 2 Configure the ONU.

NOTE

The management VLAN and the management IP address have been configured. Therefore, you can run the **telnet** ***192.168.50.2*** command on the OLT to log in to the ONU and configure the ONU. You can also log in to the ONU through a serial port and configure it.

1. Log in to the ONU and configure it.

   On the OLT, use the management IP address of the ONU to log in to the ONU in telnet mode. The user name is **root** (default) and its default password is **mduadmin**.

   ```
   huawei(config)#telnet 192.168.50.2
   { <cr>|service-port<U><0,4294967295> }:

     Command:
             telnet 192.168.50.2
     Press CTRL_] to quit telnet mode
     Trying 192.168.50.2 ...
     Connected to 192.168.50.2 ...
   >>User name:root
   >>User password:      //It is not displayed on the console.
   ```

2. Configure a VLAN Layer 3 interface.

   Configure the service VLAN ID to 30 and VLAN type to smart, add uplink port 0/0/0 to VLAN 30, and set the IP address of the Layer 3 interface to 10.1.1.3.

Copyright © Huawei Technologies Co., Ltd.

```
huawei(config)#vlan 30 standard
huawei(config)#port vlan 30 0/0 0
huawei(config)#interface vlanif 30
huawei(config-if-vlanif30)#ip address 10.1.1.3 24
huawei(config-if-vlanif30)#quit
```

3. Configure the serial port working mode.

   Configure the serial port working mode to RS485, which is the same as the working mode of the serial port on the terminal unit.

   ```
   huawei(config)#interface serial 0/2
   huawei(config-if-serial-0/2)#port mode 0 rs485
   ```

4. (Optional) Configure serial port attributes.

   The default value of the serial port baud rate is 2400 bit/s. Configure the serial port baud rate to be the same as the baud rate of the serial port on the terminal unit.

   ```
   huawei(config)#interface serial 0/2
   huawei(config-if-serial-0/2)#port config 0 baudrate 2400
   ```

5. Configure a serial port connection.

   Configure the data transmission mode to **TCP Server**, local end IP address for the TCP/IP connection to 10.1.1.3, local port ID to 3000, peer end IP address for the TCP/IP connection to 10.1.1.2, and serial port frame type to none.

   ```
   huawei(config)#serialop-connection 1 port 0/2/0 working-mode tcp-server local-address
    10.1.1.3 local-port 3000 peer-address 10.1.1.2 frame-type none
   ```

6. Save the data.

   ```
   huawei(config)#save
   ```

----End

Result

1. Run the **ping** command to verify that the route between the ONU and the master station server is available.
2. Run the **display serialop-connection** command to query whether the status of the serial port TCP/IP connection is **established** to determine whether the ONU and the master station server communicate with each other properly.

   NOTE

   If **working-mode** of the serial port connection is **TCP-Client**, run the **display serialop-connection** command to query whether the status of the serial port TCP/IP connection is **connected** to determine whether the ONU and the master station server communicate with each other properly.

   If **working-mode** of the serial port connection is **UDP**, run the **display serialop-connection statistics** command to query the number of frames received on or sent from the serial port to determine whether the ONU and the master station server communicate with each other properly.

Configuration File

The OLT configurations are as follows:

```
vlan 30 smart
port vlan 30 0/19 0
vlan 8 smart
port vlan 8 0/19 0
```


Copyright © Huawei Technologies Co., Ltd.

```
interface vlanif 8
ip address 192.168.50.10 24
quit
dba-profile add profile-name SerialAccess type3 assure 20480 max 51200
ont-lineprofile gpon profile-id 10
tcont 5 dba-profile-name SerialAccess
gem add 0 eth tcont 5 priority-queue 3
gem add 1 eth tcont 5 priority-queue 3
mapping-mode vlan
gem mapping 0 0 vlan 8
gem mapping 1 1 vlan 30
commit
quit
interface gpon 0/3
port 1 ont-auto-find enable
ont confirm 1 ontid 1 sn-auth 48575443E6D8B541 snmp ont-lineprofile-id
 10 desc MA5621_0/3/1/1_lineprofile10
ont ipconfig 1 1 static ip-address 192.168.50.2 mask 255.255.255.0 vlan 8
ont alarm-profile 1 1 profile-id 1
service-port 0 vlan 8 gpon 0/3/1 ont 1 gemport 0 multi-service
user-vlan 8 rx-cttr 6 tx-cttr 6
traffic table ip index 20 cir off priority 1 priority-policy local-Setting
service-port 1 vlan 30 gpon 0/3/1 ont 1 gemport 1 multi-service
user-vlan 30 rx-cttr 20 tx-cttr 20
queue-scheduler wrr 10 10 20 20 40 0 0 0
cos-queue-map cos0 0 cos1 1 cos2 2 cos3 3 cos4 4 cos5 5 cos6 6 cos7 7
save
```

The ONU configurations are as follows:

```
vlan 30 standard
port vlan 30 0/0 0
interface vlanif 30
ip address 10.1.1.3 24
quit
interface serial 0/2
port mode 0 rs485
interface serial 0/2
port config 0 baudrate 2400
serialop-connection 1 port 0/2/0 working-mode tcp-server local-address
 10.1.1.3 local-port 3000 peer-address 10.1.1.2 frame-type none
save
```


Copyright © Huawei Technologies Co., Ltd.

18 OptiCable EoC Bandwidth Configuration

About This Chapter

The OptiCable solutions mainly apply to two scenarios: bidirectional restructuring for existing cable TV users, and cable TV and broadband service access over coaxial cables for new users. The radio frequency (RF) access can be deployed in a network to support both passive optical network (PON) and ethernet over coaxial cable (EoC) services. Such a network scenario supports high-speed Internet (HSI) and Internet protocol television (IPTV) services, meeting broadcast and television services requirements.

18.1 Configuring Example of EoC Services (OLTs Use GPON Access)
Ethernet over coaxial cable (EoC) is a key technology for the next-generation broadcast and TV networks. This technology can be used to reconstruct the existing cable networks to bidirectional broadband network to provide bandwidth services such as high-speed Internet (HSI) and Internet protocol television (IPTV). This topic uses the MA5631 as an optical network unit (ONU) to describe how to configure EoC broadband services.

Copyright © Huawei Technologies Co., Ltd.

18.1 Configuring Example of EoC Services (OLTs Use GPON Access)

Ethernet over coaxial cable (EoC) is a key technology for the next-generation broadcast and TV networks. This technology can be used to reconstruct the existing cable networks to bidirectional broadband network to provide bandwidth services such as high-speed Internet (HSI) and Internet protocol television (IPTV). This topic uses the MA5631 as an optical network unit (ONU) to describe how to configure EoC broadband services.

Service Requirements

Users can subscribe to broadcast and TV services, Internet access services, and interaction services. Broadcast and TV services can be provided after the ONU hardware is connected and the service channel is set up. No configuration is required. This topic only describes how to configure the Internet access and interaction services.

The CNU uses the HG7022, providing two LAN ports. Port 1 is connected to a PC for providing the Internet access service and port 2 is connected to a set top box (STB) for providing a return channel for the interactive TV service. The CNU differentiates services by port. Virtual local area networks (VLANs) are not switched on the optical line terminal (OLT) and services are transparently transmitted on the OLT.

- Users access the Internet in Point-to-Point Protocol over Ethernet (PPPoE) dialup mode.
- Policy Information Transfer Protocol (PITP) is enabled to protect user accounts against theft and roaming.

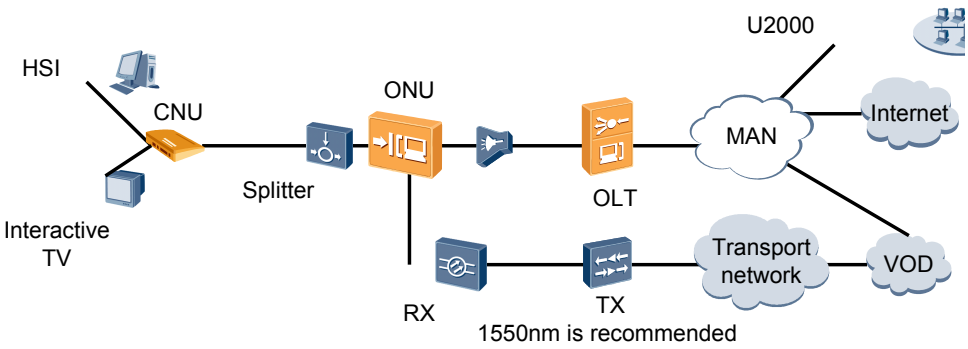
  NOTE

  In Dynamic Host Configuration Protocol (DHCP) dialup mode, you can configure anti-theft and roaming for user accounts. For details, see **Configuring Anti-Theft and Roaming for User Accounts Using DHCP**.

Networking

Figure 18-1 shows a network diagram of the EoC broadband service.

Figure 18-1 Network diagram of the EoC broadband service



Copyright © Huawei Technologies Co., Ltd.

Data Plan

Table 18-1 provides the data plan for the OLT, and Table 18-2 provides the data plan for the ONU.

Table 18-1 Data plan for configuring the EoC broadband service-OLT side

Item	Data
VLAN	Inband management VLAN: smart VLAN 8 SVLAN: smart VLAN 100 with the attribute Common SVLAN: smart VLAN 101 with the attribute Common
IP address	Inband management IP address: 192.168.50.1/24
GPON service board	Port ID: 0/3/1 ONU ID: 1 ONU authentication mode: SN ONU SN: 48575443E6D8B541
DBA profile	Profile name: PrivateLine Type: type3 Assured bandwidth: 20 Mbit/s Maximum bandwidth: 50 Mbit/s
ONU line profile	Profile ID: 10, bound to the DBA profile named PrivateLine GEM port IDs: 0, 1, and 2 T-CONT ID: 5
ONU management mode	SNMP

Table 18-2 Data plan for configuring the EoC broadband service-ONU side

Item	Data
CNU	● CNU ID: 0 ● CNU MAC address: 00B0-5240-0003 ● CNU SN: hwhw-12341234 ● CNU line profile: 1
VLAN	Inband management VLAN: smart VLAN 8, adding GPON upstream port 0/0/0 to this VLAN HSI SVLAN: smart VLAN 100 with the attribute Stacking, adding GPON upstream port 0/0/0 to the VLAN Interactive TV SVLAN: smart VLAN 101 with the attribute Common, adding GPON upstream port 0/0/0 to the VLAN

Copyright © Huawei Technologies Co., Ltd.

Item	Data
IP address	Inband management IP address: 192.168.50.2/24

Procedure

Step 1 Configure the OLT.

1. Create an SVLAN and add an upstream port to it.

   Create smart VLANs 100 and 101, their attributes are common, and add upstream port 0/19/0 to the VLANs.

   ```
   huawei(config)#vlan 100-101 smart
   huawei(config)#vlan attrib 100 common
   huawei(config)#vlan attrib 101 common
   huawei(config)#port vlan 100-101 0/19 0
   ```

2. (Optional) Configure upstream link aggregation.

   In this example, a single upstream port is used. In the case of multiple upstream ports, configure upstream link aggregation. For details, see "Configuring the Link Aggregation of Upstream Ethernet Port".

3. Configure GPON ONU profiles.

   GPON ONU profiles include the DBA profile, line profile, service profile, and alarm profile.

   - DBA profile: A DBA profile describes the GPON traffic parameters. A T-CONT is bound to a DBA profile for dynamic bandwidth allocation, improving the upstream bandwidth usage.
   - Line profile: A line profile describes the binding between the T-CONT and the DBA profile, the QoS mode of the traffic stream, and the mapping between the GEM port and the ONU-side service.
   - Service profile: A service profile provides the service configuration channel for the ONU that is managed using optical network terminal management and control interface (OMCI).
   - Alarm profile: An alarm profile contains a series of alarm thresholds to measure and monitor the performance of activated ONU lines. When a statistical value reaches the threshold, the host is notified and an alarm is reported to the log host and the NMS.

   a. Add a DBA profile.

      Run the **display dba-profile** command to query the DBA profiles in the system. If the DBA profiles in the system do not meet requirements, run the **dba-profile add** command to add a DBA profile.

      Configure the profile name to PrivateLine, profile type to Type3, assured bandwidth to 20 Mbit/s, and maximum bandwidth to 50 Mbit/s.

      ```
      huawei(config)#dba-profile add profile-name PrivateLine type3 assure
      20480 max 51200
      ```

   b. Add an ONU line profile.

      Add GPON ONU line profile 10 and bind T-CONT 5 to the DBA profile named PrivateLine. In this way, the T-CONT can provide flexible DBA solutions based on different configurations in the DBA profile.

Copyright © Huawei Technologies Co., Ltd.

```
huawei(config)#ont-lineprofile gpon profile-id 10
huawei(config-gpon-lineprofile-10)#tcont 5 dba-profile-name PrivateLine
```

Add GEM port 0 for transmitting management traffic streams, GEM port 1 for transmitting HSI traffic streams and GEM port 2 for transmitting interactive TV traffic streams. Bind GEM port 0, GEM port 1 and GEM port 2 to T-CONT 5. Configure the QoS mode to priority-queue (default) and the queue priority to 3.

NOTE

1. To change the QoS mode, run the **qos-mode** command to configure the QoS mode to gem-car or flow-car, and run the gem add command to configure the ID of the traffic profile bound to the GEM port.
2. When the QoS mode is PQ, the default queue priority is 0; when the QoS is flow-car, traffic profile 6 is bound to the port by default (no rate limitation); when the QoS mode is gem-car, traffic profile 6 is bound to the port by default (no rate limitation).

huawei(config-gpon-lineprofile-10)#**gem add 0 eth tcont 5 priority-queue 3**

huawei(config-gpon-lineprofile-10)#**gem add 1 eth tcont 5 priority-queue 3**

huawei(config-gpon-lineprofile-10)#**gem add 2 eth tcont 5 priority-queue 3**

Configure the mapping mode from the GEM port to ONU-side service to VLAN (default), map the service port of management VLAN 8 to GEM port 0, map the service port of HSI SVLAN 100 to GEM port 1 and map the service port of the interactive TV SVLAN 101 to GEM port 2.

```
huawei(config-gpon-lineprofile-10)#mapping-mode vlan
huawei(config-gpon-lineprofile-10)#gem mapping 0 0 vlan 8
huawei(config-gpon-lineprofile-10)#gem mapping 1 1 vlan 100
huawei(config-gpon-lineprofile-10)#gem mapping 2 2 vlan 101
```

After the configuration is complete, run the **commit** command to make the configured parameters take effect.

```
huawei(config-gpon-lineprofile-10)#commit
huawei(config-gpon-lineprofile-10)#quit
```

(Optional) Add an alarm profile.

- The ID of the default GPON alarm profile is 1. The thresholds for all the alarm parameters in the default alarm profile are 0, which indicates that no alarm is generated.
- In this example, the default alarm profile is used, and therefore the configuration of the alarm profile is not required.
- Run the **gpon alarm-profile add** command to add an alarm profile, which is used for monitoring the performance of an activated ONU line.

4. Add an ONU on the OLT.

The ONU is connected to the GPON port of the OLT using an optical fiber. You can perform the service configuration only after adding an ONU successfully on the OLT.

a. Add an ONU.

Connect the ONU to GPON port 0/3/1. The ONU ID is 1, the serial number (SN) is 48575443E6D8B541, the management mode is SNMP, and the bound line profile ID is 10.

Add an ONU in either of the following two methods based on site requirements:

- Add an ONU offline: If the password or SN of an ONU is obtained, you can run the **ont add** command to add the ONU offline.

Copyright © Huawei Technologies Co., Ltd.

- Find an ONU automatically: If the password or SN of an ONU is unknown, run the port ont-auto-find command in GPON mode to enable the ONU auto-find function of the GPON port. Then run the **ont confirm** command to confirm the ONU.

To add an ONU offline, do as follows:

```
huawei(config)#interface gpon 0/3
huawei(config-if-gpon-0/3)#ont add 1 1 sn-auth 48575443E6D8B541 snmp ont-
lineprofile-id
 10 desc MA5631_0/3/1/1_lineprofile10
```

To automatically find an ONU, do as follows:

```
huawei(config)#interface gpon 0/3
huawei(config-if-gpon-0/3)#port 1 ont-auto-find enable
huawei(config-if-gpon-0/3)#display ont autofind 1
   //After this command is executed, the information about all the ONUs
connected to
  //the GPON port using the optical splitter is displayed.

   ------------------------------------------------------------
   Number              : 1
   F/S/P               : 0/3/1
   Ont SN              : 48575443E6D8B541
   Password            :
   VenderID            : HWTC
   Ont Version         : MA5631
   Ont SoftwareVersion : V800R310C00
   Ont EquipmentID     : SmartAX MA5631
   Ont autofind time   : 2011-09-10 11:20:16
   ------------------------------------------------------------
huawei(config-if-gpon-0/3)#ont confirm 1 ontid 1 sn-auth 48575443E6D8B541
snmp ont-lineprofile-id
 10 desc MA5631_0/3/1/1_lineprofile10
```

NOTE

If multiple ONUs of the same type are connected to a port and the same line profiles or service profiles are bound to the ONUs, add these ONUs in batches by confirming the auto-found ONUs in batches. The adding simplifies the operation and increases the configuration efficiency. Therefore, the preceding command can be modified to: huawei(config-if-gpon-0/3)#**ont confirm 1 all sn-auth snmp ont-lineprofile-id 10 desc MA5631_0/3/1/1_lineprofile10**.

5. Confirm that the ONU goes online properly.

After an ONU is added, run the **display ont info** command to query the ONU status. Ensure that **Control flag** of the ONU is **active**, **Run State** is **online**, and **Config state** is **normal**.

```
huawei(config-if-gpon-0/3)#display ont info 1 1

------------------------------------------------------------------------
  F/S/P                :
0/3/1
  ONT-ID               :
1
  Control flag         : active    //Indicates that the ONU is
activated.
  Run state           : online    //Indicates that the ONU already goes online
properly.
  Config state         : normal    //Indicates that the configuration status
of the ONU is normal.
...//The rest of the response information is omitted.
huawei(config-if-gpon-0/3)#quit
```

If the ONU configuration fails or the ONU fails to be up, check the ONU state by referring to the above-mentioned descriptions.

Copyright © Huawei Technologies Co., Ltd.

- If **Control flag** is **deactive**, run the **ont activate** command in GPON port mode to activate the ONU.
- If **Run state** is **offline**, the ONU fails to be up. The physical line may be broken or the optical module may be damaged. Check both the materials and line.
- If **Config state** is **failed**, the ONU configuration fails. The ONU capability set outmatches the actual ONU capabilities. Run the **display ont failed-configuration** command in diagnosis mode to check the failed configuration item and the failure cause. Then rectify the fault according to actual conditions.

  NOTE

  If an ONT supports only four queues, the values of 4–7 of the priority-queue parameter in the gem add command are invalid. After configuration recovers, **Config state** will be failed.

6. Configure the management channel from the OLT to the ONU.

   NOTE

   The management channel needs to be configured only when the OLT remotely manages the ONU using the SNMP protocol. When the OLT remotely manages the ONU using the OMCI, the management channel need not be configured.

   a. Configure the inband management VLAN and IP address of the OLT.

      To remote log in to the ONU and configure the ONU from the OLT, configure the inband management VLANs and IP addresses of the OLT and the ONU on the OLT.

      Create management VLAN 8 and set the inband management IP address to 192.168.50.1/24.

      ```
      huawei(config)#vlan 8 smart
      huawei(config)#port vlan 8 0/19 0
      huawei(config)#interface vlanif 8
      huawei(config-if-vlanif8)#ip address 192.168.50.1 24
      huawei(config-if-vlanif8)#quit
      ```

   b. Configure the inband management VLAN and IP address of the ONU.

      Set the static IP address of the ONU to 192.168.50.2/24 and the management VLAN ID to 8 (the same as the management VLAN of the OLT).

      ```
      huawei(config)#interface gpon 0/3
      huawei(config-if-gpon-0/3)#ont ipconfig 1 1 static ip-address
      192.168.50.2 mask 255.255.255.0 vlan 8
      ```

   c. Configure an inband management service port.

      Set the management service port ID to 0, management VLAN ID to 8, GEM port ID to 0, and CVLAN ID to 8. The rate of the inband service port on the OLT is not limited. Therefore, use traffic profile 6 (default). To limit the rate of the service port, run the **traffic table ip** command to add a traffic profile and bind it to the service port.

      ```
      huawei(config)#service-port 0 vlan 8 gpon 0/3/1 ont 1 gemport 0 multi-
      service
      user-vlan 8 rx-cttr 6 tx-cttr 6
      ```

7. Confirm that the management channel between the OLT and the ONU is available.
   - On the OLT, run the **ping *192.168.50.2*** command to check the connectivity to the ONU. ICMP ECHO-REPLY packets from the ONU should be received.
   - You can remote log in to the ONU from the OLT to perform the configuration.
8. Create a service port.

   Configure the port ID of the HSI service to 1, SVLAN ID to 100, GEM port ID to 1, CVLAN ID to 100, and configure the port ID of the interactive TV service to 2, SVLAN ID to 101, GEM port ID to 2, CVLAN ID to 101. Rate limitation for upstream and downstream packets

Copyright © Huawei Technologies Co., Ltd.

is performed on the MDU instead of on the OLT. Therefore, use traffic profile 6 (default). To limit the rate of the service port, run the **traffic table ip** command to add a traffic profile and bind it to the service port.

The CVLAN must be the same as the upstream VLAN of the ONU.

```
huawei(config)#service-port 1 vlan 100 gpon 0/3/1 ont 1 gemport 1 multi-
service
user-vlan 100 rx-cttr 6 tx-cttr 6
huawei(config)#service-port 2 vlan 101 gpon 0/3/1 ont 1 gemport 2 multi-
service
user-vlan 101 rx-cttr 6 tx-cttr 6
```

9. Configure queue scheduling.

   Use the 3PQ+5WRR queue scheduling. Queues 0-4 use the WRR mode, with the weights of 10, 10, 20, 20, and 40 respectively; queues 5-7 use the PQ mode. The service priority is 4, using the WRR scheduling.

   Queue scheduling is a global configuration. Configure queue scheduling on the OLT only once, and then the configuration takes effect globally. In subsequent service configurations, you do not need to configure queue scheduling.

   ```
   huawei(config)#queue-scheduler wrr 10 10 20 20 40 0 0 0
   ```

   Configure the mapping between queues and 802.1p priorities. Priorities 0-7 map queues 0-7 respectively.

   For the service board that supports only four queues, the mappings between 802.1p priorities and queue IDs are as follows: priorities 0 and 1 map queue 1; priorities 2 and 3 map queue 2; priorities 4 and 5 map queue 3; priorities 6 and 7 map queue 4.

   ```
   huawei(config)#cos-queue-map cos0 0 cos1 1 cos2 2 cos3 3 cos4 4 cos5 5 cos6 6
   cos7 7
   ```

10. Save the data.

    ```
    huawei(config)#save
    ```

Step 2 Configure the ONU to provide services automatically.

The CNU can automatically provide services after going online. No additional service configuration operation is required and therefore the service provisioning efficiency is improved.

NOTE

Because the management VLAN and the management IP address have been configured, you can remote log in to the ONU from the OLT to perform the configuration.

1. Log in to the ONU to perform the configuration.

   On the OLT, you can remote log in to the ONU to perform the configuration. The user name is **root** (default) and the password is **mduadmin** (default).

2. Confirm an automatically discovered CNU.

   Services are automatically provided after the CNU is automatically discovered.

   ```
   huawei(config)#interface eoc 0/1
   huawei(config-if-eoc-0/1)#cnu auto confirm all
   ```

3. Create an SVLAN.

   Set the VLAN ID of the HSI service to 100, the VLAN type to smart, and the attribute to stacking, and add uplink port 0/0/0 to this VLAN. Set the VLAN ID of the interactive TV service to 101, the VLAN type to smart, and the attribute to common, and add uplink port 0/0/0 to this VLAN.

Copyright © Huawei Technologies Co., Ltd.

```
huawei(config)#vlan 100-101 smart
huawei(config)#vlan attrib 100 stacking
huawei(config)#vlan attrib 101 common
huawei(config)#port vlan 100-101 0/0 0
```

4. Create a profile for automatic service provisioning by the CNU.

   Configure the HSI service profile ID to 1, service VLAN ID to 100, CNU port ID to 1, and traffic profile to 3.

   ```
   huawei(config)#cnu auto-service-profile add 1 vlan 100 eth 1 inbound traffic-table index 3 outbound traffic-table index 3
   ```

   Configure the interactive TV service profile ID to 1, service VLAN ID to 100, CNU port ID to 1, and traffic profile to 3.

   ```
   huawei(config)#cnu auto-service-profile add 1 vlan 101 eth 2 inbound traffic-table index 4 outbound traffic-table index 4
   ```

Step 3 Configure the ONU to provide services through manual operations.

Users must manually configure services after the CNU goes online.

NOTE

Because the management VLAN and the management IP address have been configured, you can remote log in to the ONU from the OLT to perform the configuration.

1. Log in to the ONU to perform the configuration.

   On the OLT, you can remote log in to the ONU to perform the configuration. The user name is **root** (default) and the password is **mduadmin** (default).

2. **Optional:** Configure a line profile for the EoC head end module.

   A line profile is generally not required for the EoC head end module because the default line profile 1 is automatically bound to the head end module port. For details about how to customize a line profile, see *Configuration Guide* of the ONU.

   The default profile is used in this example.

3. **Optional:** Configure a CNU line profile.

   A CNU line profile is generally not required because the default line profile 1 is automatically bound to the CNU. For details about how to customize a line profile, see *Configuration Guide* of the ONU.

   The default profile is used in this example.

4. Add a CNU to an ONU.

   Assume that a CNU ID is 0, the CNU SN is hwhw-12341234, the bound line profile is 1, the description added to the CNU is huaweicnu, and the CNU alarm reporting function is disabled by default. To connect this CNU to EoC head end module port 0/1/0, you can use two methods: add a CNU offline and confirm an automatically discovered CNU.

   - Add an CNU offline.

     If the CNU SN is known, run the **cnu add** command to add the CNU offline.

     ```
     huawei(config)#interface eoc 0/1
     huawei(config-if-eoc-0/1)#cnu add 0 0 sn-auth hwhw-12341234 lineprofile-id 1
     desc huaweicnu
     huawei(config-if-eoc-0/1)#quit
     ```


Copyright © Huawei Technologies Co., Ltd.

- Confirm an automatically discovered CNU.

  If the CNU SN is unknown, run the **cnu auto confirm** command in EoC mode to enable the CNU automatic discover function on the EoC port.

```
huawei(config)#interface eoc 0/1
huawei(config-if-eoc-0/1)#cnu auto confirm all
```

5. Create an SVLAN.

   Set the VLAN ID of the HSI service to 100, the VLAN type to smart, and the attribute to stacking, and add uplink port 0/0/0 to this VLAN. Set the VLAN ID of the interactive TV service to 101, the VLAN type to smart, and the attribute to common, and add uplink port 0/0/0 to this VLAN.

```
huawei(config)#vlan 100-101 smart
huawei(config)#vlan attrib 100 stacking
huawei(config)#vlan attrib 101 common
huawei(config)#port vlan 100-101 0/0 0
```

6. Configure the traffic profile.

   Run the **display traffic table ip** command to query the traffic profiles in the system. If the traffic profiles in the system do not meet requirements, run the **traffic table ip** command to add a traffic profile. This example uses the default traffic profile.

```
huawei(config)#display traffic table ip from-index
0
{ <cr>|to-
index<K> }:


Command:
          display traffic table ip from-index
0

------------------------------------------------------------------------------
   TID CIR(kbps) CBS(bytes) PIR(kbps) PBS(bytes) Pri Copy-policy    Pri-
Policy

------------------------------------------------------------------------------
     0       512      18384      1024      36768   6 -             tag-
pri
     1      1024      34768      2048      69536   0 -             tag-
pri
     2      2048      67536      4096     135072   0 -             tag-
pri
     3      4096     133072      8192     266144   4 -             tag-
pri
     4      8192     264144     16384     528288   4 -             tag-
pri
     5     16384     526288     32768    1024000   4 -             tag-
pri
     6       off        off       off        off   0 -             tag-
pri

------------------------------------------------------------------------------
  Total Num : 7
```

7. Create a service port and bind it to a traffic profile.

   VLAN tags are switched for the HSI service. The outer VLAN tag, or SVLAN tag, identifies OLT+PON port+services, and the inner VLAN tag, or CVLAN tag, identifies CNU+ONU ID.

```
huawei(config)#service-port 1 vlan 100 eoc 0/1/0 cnu 0 eth 1 multi-service
user-
vlan untagged inbound traffic-table index 3 outbound traffic-table index 3
huawei(config)#stacking label service-port 100 2
```


Copyright © Huawei Technologies Co., Ltd.

CVLAN to SVLAN tag switching is performed for the interactive TV service. The S-VLAN identifies services.

```
huawei(config)#service-port 2 vlan 101 eoc 0/1/0 cnu 0 eth 2 multi-service
user-
vlan untagged inbound traffic-table index 4 outbound traffic-table index 4
```

8. Configure the user account security.

   The PITP P mode can be enabled to protect the user account against theft and roaming.

   ```
   huawei(config)#pitp enable pmode
   ```

   NOTE

   For details about the PITP configuration for the user account security, see **Configuring Anti-Theft and Roaming of User Account Using PITP**.

9. Save the data.

   ```
   huawei(config)#save
   ```

----End

Result

- The users connected to port 1 on the CNU can use the HSI service.
- The users connected to port 2 on the CNU can use the interactive TV service.

NOTE

The users connected to LAN ports can use the Internet access service or interactive TV service based on requirements, regardless of whether the CNU provides two or four ports. The procedure for configuring the EoC broadband services on the CNU with four ports is the same as the preceding procedure for configuring the EoC broadband services on the CNU with two ports.

Configuration File

Configure the OLT.

```
vlan 100-101 smart
vlan attrib 100 common
vlan attrib 101 common
port vlan 100-101 0/19 0
vlan 8 smart
port vlan 8 0/19 0
interface vlanif 8
ip address 192.168.50.1 24
quit
dba-profile add profile-name PrivateLine type3 assure 20480 max 51200
ont-lineprofile gpon profile-id 10
tcont 5 dba-profile-name PrivateLine
gem add 0 eth tcont 5 priority-queue 3
gem add 1 eth tcont 5 priority-queue 3
gem add 2 eth tcont 5 priority-queue 3
mapping-mode vlan
gem mapping 0 0 vlan 8
gem mapping 1 1 vlan 100
gem mapping 2 2 vlan 101
commit
quit
interface gpon 0/3
port 1 ont-auto-find enable
display ont autofind 1
ont confirm 1 ontid 1 sn-auth 48575443E6D8B541 snmp ont-lineprofile-id
 10 desc MA5631_0/3/1/1_lineprofile10
ont ipconfig 1 1 static ip-address 192.168.50.2 mask 255.255.255.0 vlan 8
ont alarm-profile 1 1 profile-id 1
```


Copyright © Huawei Technologies Co., Ltd.

```
service-port 0 vlan 8 gpon 0/3/1 ont 1 gemport 0 multi-service
user-vlan 8 rx-cttr 6 tx-cttr 6
service-port 1 vlan 100 gpon 0/3/1 ont 1 gemport 1 multi-service
user-vlan 100 rx-cttr 6 tx-cttr 6
service-port 2 vlan 101 gpon 0/3/1 ont 1 gemport 2 multi-service
user-vlan 101 rx-cttr 6 tx-cttr 6
queue-scheduler wrr 10 10 20 20 40 0 0 0
cos-queue-map cos0 0 cos1 1 cos2 2 cos3 3 cos4 4 cos5 5 cos6 6 cos7 7
save
```

Configure the ONU to provide services automatically.

```
interface eoc 0/1
cnu auto confirm all
vlan 100-101 smart
port vlan 100-101 0/0 0
cnu auto-service-profile add 1 vlan 100 eth 1 inbound traffic-table index 3
outbound traffic-table index 3
cnu auto-service-profile add 1 vlan 101 eth 2 inbound traffic-table index 4
outbound traffic-table index 4
```

Configure the ONU to provide services through manual operations.

```
interface eoc 0/1
cnu add 0 0 sn-auth hwhw-12341234 lineprofile-id 1
desc huaweicnu
quit
vlan 100-101 smart
port vlan 100-101 0/0 0
vlan service-profile profile-id 1
vlan service-profile profile-id 2
commit
quit
vlan bind service-profile 100 profile-id 1
vlan bind service-profile 101 profile-id 2
service-port 1 vlan 100 eoc 0/1/0 cnu 0 eth 1 multi-service user-
vlan untagged inbound traffic-table index 3 outbound traffic-table index 3
service-port 2 vlan 101 eoc 0/1/0 cnu 0 eth 2 multi-service user-
vlan untagged inbound traffic-table index 4 outbound traffic-table index 4
pitp enable pmode
save
```


Copyright © Huawei Technologies Co., Ltd.

19 IPv6 Configuration

About This Chapter

19.1 IPv6 Networking
The FTTH IPv6 solution is part of the Huawei fixed broadband solution for IPv6, supporting the access of the IPv6 high speed Internet (HSI) service and IPTV service.

19.2 Configuration Difference Between IPv6 and IPv4
The main configuration difference between the IPv6 and IPv4 services lies in the configurations on the OLT, MDU, and ONT.

19.3 Configuring IPv6 Services in the FTTB/C (No HGWs) Scenario
This section describes the methods for configuring IPv6 services in the FTTB/C (No HGWs) scenario.

19.4 Configuring IPv6 Services in the FTTB+HGW Scenario
This section describes the methods for configuring IPv6 services in the FTTB+HGW scenario.

19.5 Configuring IPv6 Services in the FTTH (Bridging ONT) Scenario
This section describes the methods for configuring IPv6 services in the FTTH (bridging ONT) scenario.

19.6 Configuring IPv6 Services in the FTTH (Gateway ONT) Scenario
This section describes the methods for configuring IPv6 services in the FTTH (gateway ONT) scenario.

Copyright © Huawei Technologies Co., Ltd.

19.1 IPv6 Networking

The FTTH IPv6 solution is part of the Huawei fixed broadband solution for IPv6, supporting the access of the IPv6 high speed Internet (HSI) service and IPTV service.

The Huawei FBB solution for IPv6 includes the following scenarios based on service access modes. Since "HSI scenario: IPv4/IPv6 DS+PPPoE+L2TP" and "HSI scenario: IPv4/IPv6 DS +NAT+PPPoE" in this solution are the same as those in the FTTx solution, they are not elaborated in this document.

- HSI scenario: IPv4/IPv6 DS+NAT+PPPoE
- HSI scenario: IPv4/IPv6 DS+NAT+IPoE
- HSI scenario: IPv4/IPv6 DS+PPPoE+L2TP
- HSI scenario: DS-Lite+PPPoE
- IPTV scenario: IPv4/IPv6 DS+IPoE
- IPTV scenario: IPv4/IPv6 DS+PPPoE

The access network devices still use IPv4, instead of IPv6, to implement voice services.

Table 19-1 lists how the access network devices process different services in different IPv6 networking scenarios. For details, see the data planning and configuration for each scenario.

Table 19-1 IPv6 networking scenarios

Network Topology	Service	Scheme	OLT	ONU
FTTB/C (no HGW)	HSI	IPv4/IPv6 DS+NAT +PPPoE	Layer 2 forwarding	Layer 2 forwarding
		IPv4/IPv6 DS+NAT +IPoE		
		DS-Lite +PPPoE	Not supported	Not supported
	IPTV	IPv4/IPv6 DS+IPoE	No such networking scenario	No such networking scenario
		IPv4/IPv6 DS +PPPoE		
FTTB +HGW	HSI	IPv4/IPv6 DS+NAT +PPPoE	Layer 2 forwarding	Layer 2 forwarding

Copyright © Huawei Technologies Co., Ltd.

Network Topology	Service	Scheme	OLT	ONU
		IPv4/IPv6 DS+NAT +IPoE		
		DS-Lite +PPPoE		
	IPTV	IPv4/IPv6 DS+IPoE	It is recommended to establish a multicast service channel from the OLT to the ONU to transparently transmit multicast service packets at Layer 2.	It is recommended to use the ONU to duplicate IPv6 multicast flows.
		IPv4/IPv6 DS +PPPoE	Not recommended	Not recommended
FTTH (bridging ONT)	HSI	IPv4/IPv6 DS+NAT +PPPoE	Layer 2 forwarding	Layer 2 forwarding
		IPv4/IPv6 DS+NAT +IPoE		
		DS-Lite +PPPoE	Not supported	Not supported
	IPTV	IPv4/IPv6 DS+IPoE	The OLT is used to duplicate IPv6 multicast flows.	Bridge forwarding
		IPv4/IPv6 DS +PPPoE	Not recommended	Not recommended
FTTH (gateway ONT)	HSI	IPv4/IPv6 DS+NAT +PPPoE	Layer 2 forwarding	To enable IPv4/IPv6 DS on the ONT, enable IPv4 and IPv6 concurrently on the WAN port.
		IPv4/IPv6 DS+NAT +IPoE		
		DS-Lite +PPPoE		If DS-Lite is enabled on the ONT, enable IPv6 and DS-Lite on the WAN port.
	IPTV	IPv4/IPv6 DS+IPoE	The OLT is used to duplicate IPv6 multicast flows.	Bridge forwarding

Copyright © Huawei Technologies Co., Ltd.

Network Topology	Service	Scheme	OLT	ONU
		IPv4/IPv6 DS +PPPoE	Not recommended	Not recommended

NOTE

In the "IPv4/IPv6 DS+PPPoE" scheme of each networking scenario, the broadband remote access server (BRAS), instead of the access network devices, duplicates multicast flows, so that this scheme does not support large scale application and is therefore not recommended.

19.2 Configuration Difference Between IPv6 and IPv4

The main configuration difference between the IPv6 and IPv4 services lies in the configurations on the OLT, MDU, and ONT.

19.2.1 Configuration Differences Between IPv6 and IPv4 on the OLT

Configurations between IPv6 and IPv4 on the OLT vary in the ACL, security feature, and IPTV multicast service.

Configuration Difference in Each Scenario

Table 19-2 lists the configuration difference between IPv6 and IPv4 on the OLT in each scenario. For details about the commands, see the later section.

Table 19-2 Configuration difference between IPv6 and IPv4 on the OLT

Service	Scheme	Configuration Difference Between IPv6 and IPv4
HSI	IPv4/IPv6 DS +NAT+PPPoE	The ACL and anti-IP spoofing configurations are different for the two services.
	IPv4/IPv6 DS +NAT+IPoE	The ACL, anti-IP spoofing, and DHCP option configurations are different for the two services.
	DS-Lite+PPPoE	The ACL and anti-IP spoofing configurations are different for the two services.
IPTV	IPv4/IPv6 DS +IPoE	The ACL, anti-IP spoofing, DHCP option, and multicast IGMP protocol configurations are different for the two services.

Copyright © Huawei Technologies Co., Ltd.

ACL

ACL configurations on the OLT are different for IPv6 and IPv4 on the network which runs both IPv4 and IPv6 services, irrespective of the networking scenarios and service implementation schemes. When configuring basic and advanced IPv6 ACLs, ensure that the keyword "ipv6" is included in the configuration command. For details, see **Table 19-3**.

Table 19-3 Commands for configuring IPv4 and IPv6 ACL on the OLT

IPv4	IPv6	IPv6 ACL Supported or Not
acl	acl ipv6	Supported
packet-filter { inbound | outbound }	packet-filter { inbound | outbound } ipv6	Supported
rule	rule	Supported **NOTE** After IPv6 is introduced, the *protocol* parameter in the rule command is extended to support the IPv6 protocols.

Security Feature

Anti-IP spoofing configurations for IPv6 and IPv4 are different on the network which runs both IPv4 and IPv6 services, irrespective of the networking scenarios and service implementation schemes. If the IPoE and DHCP protocols are used, DHCP option configurations for IPv6 and IPv4 are also different. For details, see **Table 19-4**.

- The IP addresses in anti-IP spoofing configurations are different for the two services.
- In the IPv4 configuration, DHCP option is DHCPv4 option 82. In the IPv6 configuration, DHCP option is DHCPv6 option 18/37.

  The DHCP option function is used together with the RAIO function, which enables the OLT to include physical information (including RID and CID) of the user, such as the subrack/slot/port. In this way, the BRAS or DHCP server is able to perform user authentication and tracing. When DHCPv4 is in use, the OLT includes RID and CID to the option 82 field. When DHCPv6 is in use, the OLT includes the RID to the option 37 field in the DHCPv6 packet and the CID to the option 18 field. The sub option 7 and sub option 9 functions of DHCPv4 option 82 are not supported by DHCPv6.

Table 19-4 Commands for configuring IPv4 and IPv6 security features on the OLT

IPv4	IPv6	IPv6 Security Supported or Not
DHCP Option		
raio-mode *mode* dhcp-option82	raio-mode *mode* dhcpv6-option	Supported

Copyright © Huawei Technologies Co., Ltd.

IPv4	IPv6	IPv6 Security Supported or Not
dhcp option82	dhcpv6 option	Supported
dhcp-option82 permit-forwarding service-port	dhcpv6-option permit-forwarding	Supported
raio sub-option	-	Not supported
dhcp sub-option7	-	Not supported
-	raio dhcpv6-option37 enterprise-num	Supported
display dhcp option82	display dhcpv6 option	Supported
display dhcp config	display dhcpv6 config	Supported
Anti-IP spoofing		
security anti-ipspoofing	security anti-ipv6spoofing	Supported
display security bind ip	display security bind ipv6	Supported

IPTV Multicast Service

The IGMP protocol configurations (used to implement the IPTV multicast service) for IPv6 and IPv4 on the OLT are different. IPv4 uses the IGMP protocol while IPv6 uses the MLD protocol (the IGMP protocol for IPv6). The IPv4 multicast service can share VLANs with the IPv6 multicast service; therefore, you can deploy the IPv6 multicast service in existing IPv4 MVLANs only by adding IPv6 multicast programs in the IPv4 MVLANs and in right profiles. The configured parameters such as the bound right profiles and MVLANs can remain unchanged. For details about the difference of the IGMP commands between the two services, see **Table 19-5**.

Table 19-5 Commands for configuring the IPv4 and IPv6 multicast services on the OLT

IPv4	IPv6	IPv6 Multicast Supported or Not
MVLAN		
igmp mode	igmp ipv6 mode	Supported
igmp match mode	igmp ipv6 match mode	Supported
igmp version	igmp ipv6 version	Supported
igmp match group	igmp ipv6 match group	Supported
display igmp config vlan	display igmp ipv6 config vlan	Supported

Copyright © Huawei Technologies Co., Ltd.

IPv4	IPv6	IPv6 Multicast Supported or Not
igmp inner-vlan	-	Not supported
igmp send global-leave	-	Not supported
Multicast user and right		
debugging igmp	debugging igmp ipv6	Supported
Preview		
igmp preview	-	Not supported
igmp preview reset count	-	Not supported
igmp preview reset record	-	Not supported
igmp preview-profile add	-	Not supported
igmp preview-profile delete	-	Not supported
igmp preview-profile modify	-	Not supported
display igmp preview user	-	Not supported
display igmp preview-profile	-	Not supported
Protocol parameter		
igmp proxy router gen-query-interval	igmp ipv6 proxy router gen-query-interval	Supported
igmp proxy router gen-response-time	igmp ipv6 proxy router gen-response-time	Supported
igmp proxy router robustness	igmp ipv6 proxy router robustness	Supported
igmp proxy router sp-query-interval	igmp ipv6 proxy router sp-query-interval	Supported
igmp proxy router sp-query-number	igmp ipv6 proxy router sp-query-number	Supported
igmp proxy router sp-response-time	igmp ipv6 proxy router sp-response-time	Supported
igmp initial-unsolicited-report interval	igmp ipv6 initial-unsolicited-report interval	Supported
igmp unsolicited-report interval	igmp ipv6 unsolicited-report interval	Supported
display igmp config vlan	display igmp ipv6 config vlan	Supported

Copyright © Huawei Technologies Co., Ltd.

IPv4	IPv6	IPv6 Multicast Supported or Not
igmp proxy router timeout	-	Not supported
Multicast additional function		
igmp leave-proxy	igmp ipv6 leave-proxy	Supported
igmp priority	igmp ipv6 priority	Supported
imgp report-proxy	igmp ipv6 report-proxy	Supported
igmp accelerator	-	Not supported
igmp echo	-	Not supported
igmp encapsulation	-	Not supported
igmp multicast-tag	-	Not supported
igmp policy	-	Not supported
igmp query-offline-user	-	Not supported
igmp user-action-report	-	Not supported
igmp mismatch	-	Not supported
display igmp policy	-	Not supported
igmp sip-gip-forward	-	Not supported
Statistics		
igmp statistic reset	igmp ipv6 statistic reset	Supported
display igmp statistic	display igmp ipv6 statistic	Supported
display multicast flow-statistic	-	Not supported
Log		
display igmp log statistic	-	Not supported

NOTE

The multicast commands that are not listed in this table are the commands shared by the IPv4 multicast and IPv6 multicast.

19.2.2 Configuration Differences Between IPv6 and IPv4 on the ONU

Configurations between IPv6 and IPv4 on the ONU vary in the ACL, security feature, and IPTV multicast service.

Copyright © Huawei Technologies Co., Ltd.

Configuration Difference in Each Scenario

Table 19-6 lists the configuration difference between IPv6 and IPv4 on the ONU in each scenario. For details about the commands, see the later section.

Table 19-6 Configuration difference between IPv6 and IPv4 on the ONU

Service	Scheme	Configuration Difference Between IPv6 and IPv4
HSI	IPv4/IPv6 DS +NAT+PPPoE	The ACL and anti-IP spoofing configurations are different for the two services.
	IPv4/IPv6 DS +NAT+IPoE	The ACL, anti-IP spoofing, and DHCP option configurations are different for the two services.
	DS-Lite+PPPoE	The ACL and anti-IP spoofing configurations are different for the two services.
IPTV	IPv4/IPv6 DS +IPoE	The ACL, anti-IP spoofing, DHCP option, and multicast IGMP protocol configurations are different for the two services.

ACL

ACL configurations on the ONU are different for IPv6 and IPv4 on the network which runs both IPv4 and IPv6 services, irrespective of the networking scenarios and service implementation schemes. When configuring basic and advanced IPv6 ACLs, ensure that the keyword "ipv6" is included in the configuration command. For details, see Table 19-7.

Table 19-7 Commands for configuring IPv4 and IPv6 ACL on the ONU

IPv4	IPv6	IPv6 ACL Supported or Not
acl	acl ipv6	Supported
packet-filter { inbound | outbound }	packet-filter { inbound | outbound } ipv6	Supported
rule	rule	Supported **NOTE** After IPv6 is introduced, the *protocol* parameter in the rule command is extended to support the IPv6 protocols.

Security

Anti-IP spoofing configurations for IPv6 and IPv4 are different on the network which runs both IPv4 and IPv6 services, irrespective of the networking scenarios and service implementation

Copyright © Huawei Technologies Co., Ltd.

schemes. If the IPoE and DHCP protocols are used, DHCP option configurations for IPv6 and IPv4 are also different. For details, see **Table 19-8**.

- The IP addresses in anti-IP spoofing configurations are different for the two services.
- In the IPv4 configuration, DHCP option is DHCPv4 option 82. In the IPv6 configuration, DHCP option is DHCPv6 option 18/37.

  In the IPv6 configuration, the DHCP option function is used together with the RAIO function, which enables the ONU to include physical information (including RID and CID) of the user, such as the subrack/slot/port. In this way, the BRAS or DHCP server is able to perform user authentication and tracing. When DHCPv4 is in use, the ONU includes RID and CID to the option 82 field. When DHCPv6 is in use, the ONU includes the RID to the option 37 field in the DHCPv6 packet and the CID to the option 18 field. The sub option 7 and sub option 9 functions of DHCPv4 option 82 are not supported by DHCPv6.

Table 19-8 Commands for configuring IPv4 and IPv6 security features on the ONU

IPv4	IPv6	IPv6 Security Supported or Not
Supports DHCP option82.		
raio-mode *mode* dhcp-option82	raio-mode *mode* dhcpv6-option	Supported
dhcp option82	dhcpv6 option	Supported
dhcp-option82 permit-forwarding service-port	dhcpv6-option permit-forwarding	Supported
raio sub-option	-	Not supported
dhcp sub-option7	-	Not supported
-	raio dhcpv6-option37 enterprise-num	Supported
display dhcp option82	display dhcpv6 option	Supported
display dhcp config	display dhcpv6 config	Supported
Anti-IP spoofing		
security anti-ipspoofing	security anti-ipv6spoofing	Supported
display security bind ip	display security bind ipv6	Supported

IPTV Multicast Service

The IGMP protocol configurations (used to implement the IPTV multicast service) for IPv6 and IPv4 on the ONU are different. IPv4 uses the IGMP protocol while IPv6 uses the MLD protocol (the IGMP protocol for IPv6). The IPv4 multicast service can share VLANs with the IPv6 multicast service; therefore, you can deploy the IPv6 multicast service in existing IPv4 MVLANs only by adding IPv6 multicast programs in the IPv4 MVLANs and in right profiles. The

Copyright © Huawei Technologies Co., Ltd.

configured parameters such as the bound right profiles and MVLANs can remain unchanged. For details about the difference in the IGMP commands for the two services, see **Table 19-9**.

Table 19-9 Commands for configuring the IPv4 and IPv6 multicast services on the ONU

IPv4	IPv6	IPv6 Multicast Supported or Not
MVLAN		
igmp mode	igmp ipv6 mode	Supported
igmp match mode	igmp ipv6 match mode	Supported
igmp version	igmp ipv6 version	Supported
igmp match group	igmp ipv6 match group	Supported
display igmp config vlan	display igmp ipv6 config vlan	Supported
igmp send global-leave	-	Not supported
Multicast user and right		
debugging igmp	debugging igmp ipv6	Supported
Preview		
igmp preview	-	Not supported
igmp preview reset count	-	Not supported
igmp preview reset record	-	Not supported
igmp preview-profile add	-	Not supported
igmp preview-profile delete	-	Not supported
igmp preview-profile modify	-	Not supported
display igmp preview user	-	Not supported
display igmp preview-profile	-	Not supported
Protocol parameter		
igmp proxy router gen-query-interval	igmp ipv6 router gen-query-interval	Supported
igmp proxy router gen-response-time	igmp ipv6 router gen-response-time	Supported
igmp proxy router robustness	igmp ipv6 router robustness	Supported
igmp proxy router sp-query-interval	igmp ipv6 router sp-query-interval	Supported

Copyright © Huawei Technologies Co., Ltd.

IPv4	IPv6	IPv6 Multicast Supported or Not
igmp proxy router sp-query-number	igmp ipv6 router sp-query-number	Supported
igmp proxy router sp-response-time	igmp ipv6 router sp-response-time	Supported
igmp initial-unsolicited-report interval	igmp ipv6 initial-unsolicited-report interval	Supported
igmp unsolicited-report interval	igmp ipv6 unsolicited-report interval	Supported
display igmp config vlan	display igmp ipv6 config vlan	Supported
igmp proxy router timeout	-	Not supported
Statistics		
igmp statistic reset	igmp ipv6 statistic reset	Supported
display igmp statistic	display igmp ipv6 statistic	Supported
display multicast flow-statistic	-	Not supported
Log		
display igmp log	-	Not supported
display igmp statistic	display igmp ipv6 statistic	Supported
Multicast additional function		
igmp leave-proxy	igmp ipv6 leave-proxy	Supported
igmp priority	igmp ipv6 priority	Supported
imgp report-proxy	igmp ipv6 report-proxy	Supported
igmp echo	-	Not supported
igmp encapsulation	-	Not supported
igmp policy	-	Not supported
igmp query-offline-user	-	Not supported
igmp user-action-report	-	Not supported
igmp mismatch	-	Not supported
display igmp policy	-	Not supported

Copyright © Huawei Technologies Co., Ltd.

NOTE

The multicast commands that are not listed in this table are the commands shared by IPv4 and IPv6 multicast services.

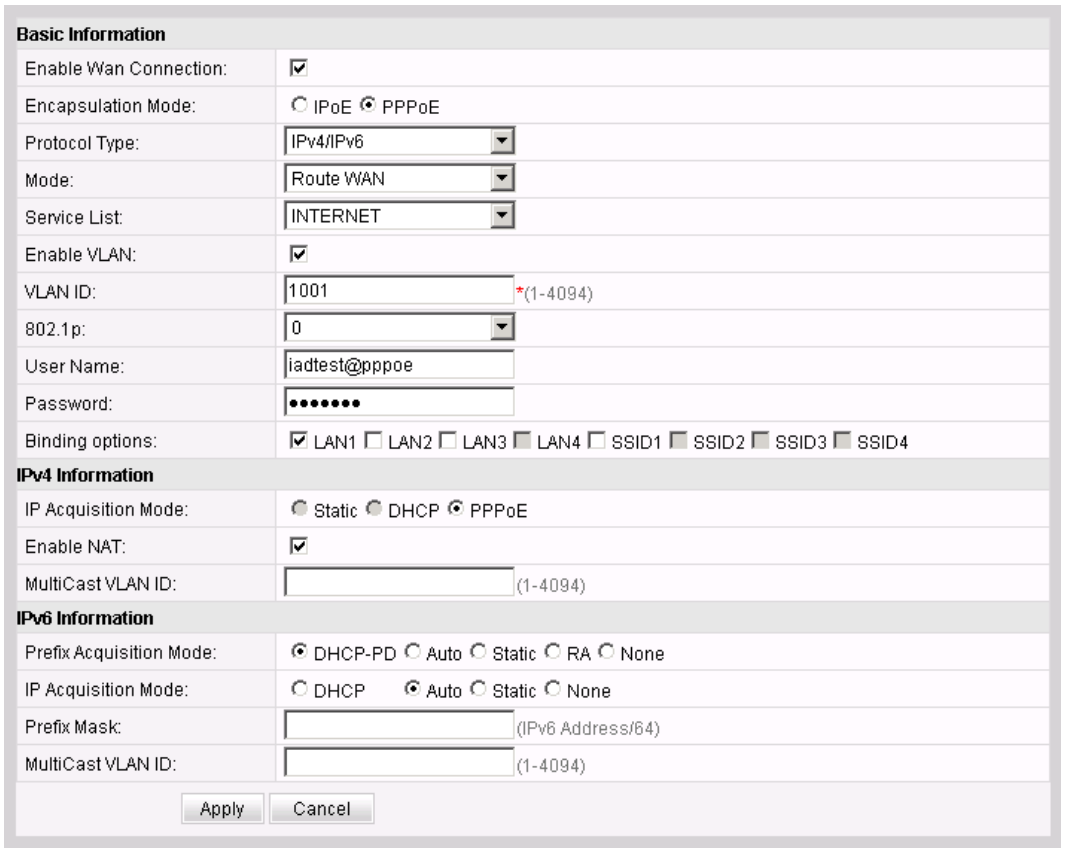
19.2.3 Configuration Difference Between IPv6 and IPv4 on the ONT

For the bridging ONT, configurations for IPv6 and IPv4 are the same. For the gateway ONT, the HSI service configurations for IPv6 and IPv4 are different.

Configuring the IPv6 WAN Port on the Gateway ONT

For IPv6 IPTV multicast service, no extra configuration is required. For the IPv6 HSI service, the Internet WAN port on the gateway ONT must be configured (only Internet WAN port supports IPv6). If the gateway ONT uses the IPv6/IPv4 DS scheme, select **IPv4/IPv6** for **Protocol Type**. If the gateway ONT uses the DS-Lite scheme, select **IPv6** for **Protocol Type**. For details, see **Figure 19-1**.

Figure 19-1 Configuring the IPv6 WAN port

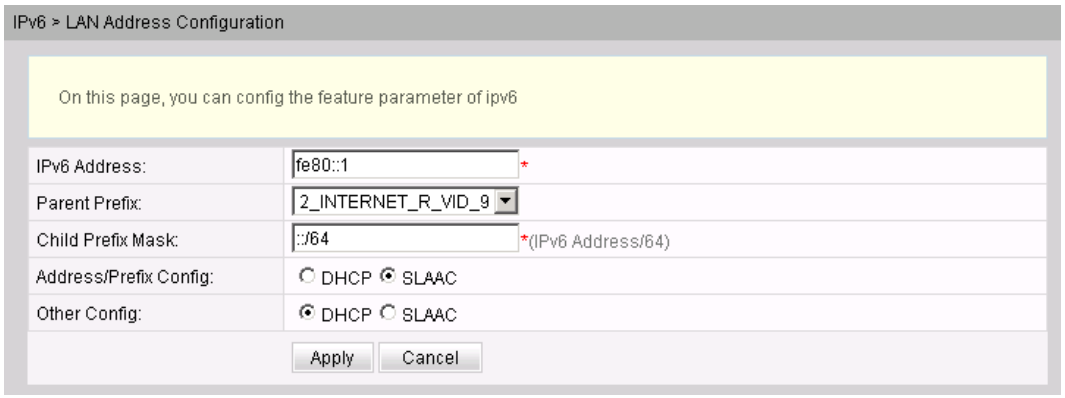


Configuring the IPv6 Address of the LAN Side on the Gateway ONT

The gateway ONT can be configured to allocate IPv6 addresses to the terminals after IPv6 is introduced. For details, see **Figure 19-2**.

Copyright © Huawei Technologies Co., Ltd.

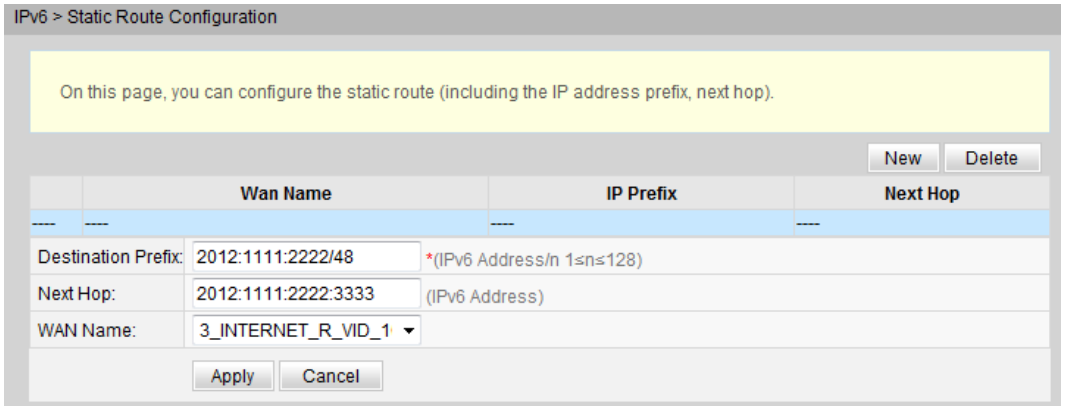
Figure 19-2 Configuring the IPv6 address on the LAN side



Configuring the Static IPv6 Route on the Gateway ONT

The gateway ONT can be configured with the static IPv6 route after IPv6 is introduced. For details, see **Figure 19-3**.

Figure 19-3 Configuring the IPv6 static route



19.3 Configuring IPv6 Services in the FTTB/C (No HGWs) Scenario

This section describes the methods for configuring IPv6 services in the FTTB/C (No HGWs) scenario.

19.3.1 Application Scenarios

The FTTB/C (no HGW) networking supports the access of IPv6 HSI services. Generally, no IPTV services will be deployed when there is no HGW.

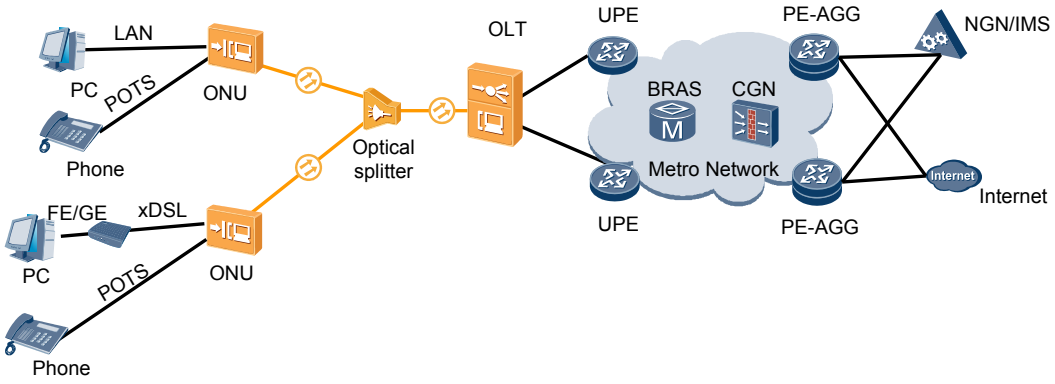
As shown in **Figure 19-4**, the ONU, which is installed in a corridor or street optical distribution box, transmits services to users through category-5 cables (LAN access) or twisted pairs (xDSL

Copyright © Huawei Technologies Co., Ltd.

access). The OLT and ONU work with upper-layer devices to support Huawei DS+NAT +PPPoE/DS+NAT+IPoE HSI IPv6 solutions.

- For voice services: The ONU with a built-in voice module can directly provide VoIP services for users. The ONU processes VoIP services using the IPv4 protocol instead of the IPv6 protocol.
- For Internet access services: Users connect to the ONU through category-5 cables (LAN access) or the modem and twisted pairs (xDSL access). The PC and BRAS support the IPv4/IPv6 DS and can be connected in the PPPoE or IPoE mode. The OLT and ONU implement Layer 2 forwarding, irrespective of whether the access service is IPv4 or IPv6. Service configurations for IPv4 and IPv6 are the same. Only the ACL, anti-IP spoofing, and DHCP option configurations for IPv4 and IPv6 are different.

Figure 19-4 FTTB/C (no HGW) networking



19.3.2 Data Planning

This section describes the security, device management data, QoS, Internet service data, and voice service data planning.

Security Planning

Security planning includes system security, user security, and service security, ensuring that user services are provided properly from different dimensions.

In the FTTB/C (no HGW) networking scenario, the data for IPv6 and IPv4 security planning differs only in anti-IP spoofing and DHCP option.

Anti-IP spoofing: This function needs to be configured separately for IPv6 services.

The anti-IP spoofing function can be enabled or disabled at three levels. This function takes effect only when it is enabled at all the three levels.

1. Global level: Run the **security anti-ipv6spoofing enable** command in global config mode.
2. VLAN level: Run the **security anti-ipv6spoofing enable** command in VLAN service profile mode.
3. Service port level: Run the **security anti-ipv6spoofing service-port** *serviceport-id* **enable** command.

Copyright © Huawei Technologies Co., Ltd.

DHCP option: The DHCP option for IPv4 is DHCPv4 option 82 and for IPv6 is DHCPv6 option 18/37.

The DHCPv6 option18 and option37 functions can be enabled or disabled at two levels. This function takes effect only when it is enabled at both levels.

1. Global level: Run the **dhcpv6 option enable** command in global config mode.
2. VLAN level: Run the **dhcpv6 option enable** command in VLAN service profile mode.

Device Management Data Planning

Device management data planning includes the management channel and IP address planning. The management channel for IPv6 and IPv4 services are the same.

Planning	Device or Service	Solution Introduction
Management channel	OLT	The device management uses single-tagged VLANs on the entire network.
	ONU	The device management uses single-tagged VLANs on the entire network.
IP address planning	Device management	IPv4 private network IP addresses are still used as management IP addresses of the OLT and MDU devices.
	Internet	● IPv4 address: A PC obtains the IPv4 address from the BRAS using PPPoE or DHCP. If IPoE dial-up is used, the static address can be configured for the PC. – The BRAS can allocate a public network IP address to a PC for Internet access. – The BRAS can allocate a private network address to a PC. The private network address is translated to the public network address by CGN (NAT44). ● IPv6 address: A PC obtains the IPv6 address from the BRAS using PPPoE, SLAAC, or DHCPv6. If IPoE dial-up is used, the static address can be configured for the PC.
	IPTV service	The IPTV service is not provisioned in this scenario.
	VoIP service	The IPv4 protocol is still used. An ONU functions as the DHCP client to obtain the IP address using DHCP.

QoS Planning

The E2E QoS planning includes the flow classification, marking/scheduling policy, traffic monitoring, and DBA policy.

Copyright © Huawei Technologies Co., Ltd.

When the IPv6 protocol is used, the QoS planning is the same for both IPv6 and IPv4.

- Management service: IPv4
- Voice service: IPv4
- IPTV service: N/A.
- Internet service: It is recommended that access devices use one flow to carry IPv6 and IPv4 Internet services. The QoS planning is the same for the flow that carries both IPv6 and IPv4 Internet services and the flow that carries only the IPv4 Internet service.

Internet Service Planning

The Internet service planning includes the VLAN and VLAN switching policy planning in different networking scenarios.

IPv6 and IPv4 Internet services: It is recommended that devices use one flow to carry IPv6 and IPv4 Internet services. This facilitates the control of the aggregate rate for IPv6 and IPv4 Internet services. The QoS planning is the same for the flow that carries both IPv6 and IPv4 Internet services and the flow that carries only the IPv4 Internet service. For details, see **11.2.3 Principle of Internet Access Service Data Plan**.

Voice Service Data Planning

Voice service data planning includes the VLAN/VLAN switching policy planning in different networking scenarios, and voice protocol planning.

Even after IPv6 is used, the device still uses IPv4 to implement voice services.

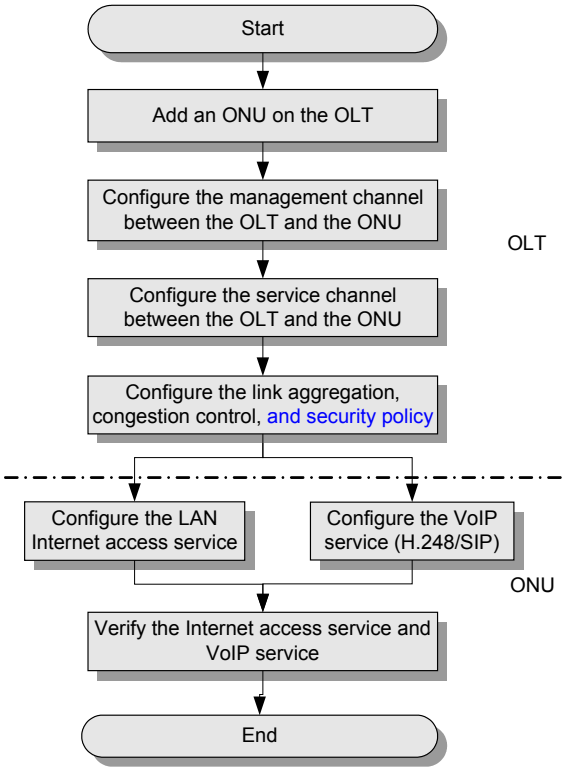
19.3.3 Configuration Procedure

This section describes the IPv6 service configuration procedure by scenario, and compares it with the IPv4 service configuration procedure.

FTTB (No HGW, LAN Access) Configuration Procedure

The following figure shows the IPv6 service configuration procedure in the FTTB (no HGW, LAN access) scenario. In this scenario, the planning and configuration procedure/method for IPv6 and IPv4 services are almost the same except the commands for configuring anti-IP spoofing and DHCP option. For details, see **19.2 Configuration Difference Between IPv6 and IPv4**.

Copyright © Huawei Technologies Co., Ltd.



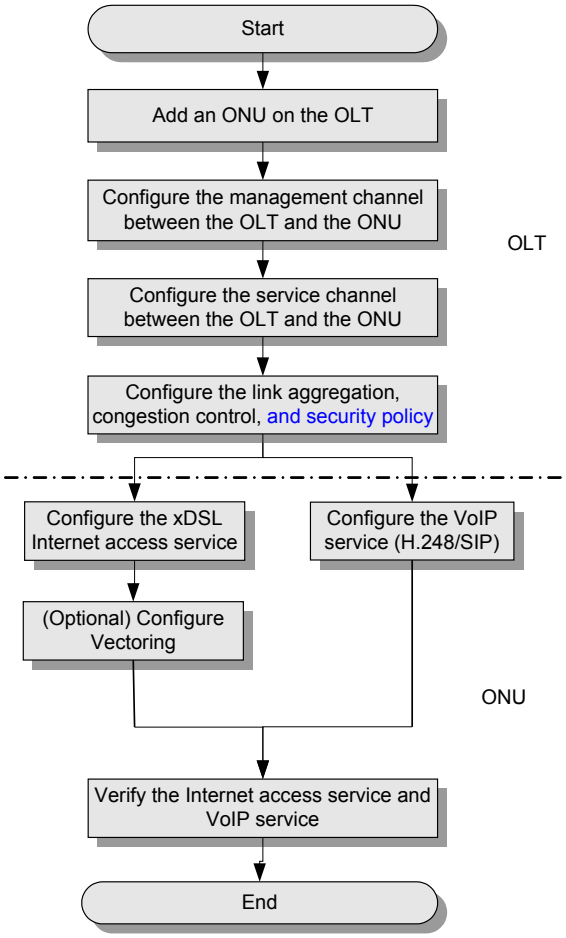
NOTE

Texts in blue show the configuration difference between IPv6 and IPv4.

FTTB/C (No HGW, xDSL Access) Configuration Procedure

The following figure shows the IPv6 service configuration procedure in the FTTB/C (no HGW, xDSL access) scenario. In this scenario, the planning and configuration procedure/method for IPv6 and IPv4 services are almost the same except the commands for configuring anti-IP spoofing and DHCP option. For details, see **19.2 Configuration Difference Between IPv6 and IPv4**.

Copyright © Huawei Technologies Co., Ltd.



NOTE

Texts in blue show the configuration difference between IPv6 and IPv4.

19.3.4 Configuration Example

Introduce the end-to-end service configuration based on the FTTB/C without HGW networking and the corresponding data plan.

Key Messages for Configuration

- Even after IPv6 is used, the OLT and ONU implement Layer 2 forwarding in this networking, irrespective of whether the access service is IPv4 or IPv6. Service configurations for IPv4 and IPv6 are the same.
- For the HSI service from one end user, one service flow is used to carry IPv6 and IPv4 Internet services, and the same service VLAN is used.
- Even after IPv6 is used, the voice service is still realized by IPv4.

Data plan on the OLT side

Item	Data	Memo
ONU data plan		

Copyright © Huawei Technologies Co., Ltd.

Item	Data	Memo
DBA profile	Profile name: fttb_dba Profile type: type3 Assured bandwidth: 8 Mbit/s Maximum bandwidth: 20 Mbit/s	The ONU is connected to OLT through the GPON interface.
Line profile	Profile name: fttb(c) Profile ID: 10 T-CONT ID: 4 GEM port ID for management service: 11 GEM port ID for Internet access service: 12 GEM port ID for VoIP service: 13	
Network topology data	PON port: 0/2/1 ONT ID: 1	
LAG data plan		
LAG	Ports: 0/19/0 and 0/19/1 Working mode: LACP static aggregation	Configure upstream ports 0/19/0 and 0/19/1 into an aggregation group. Each member port in the aggregation group allocates packets based on the source MAC address.
Queue scheduling data plan		
Queue scheduling	Queue scheduling: strict priority (SQ) mode Priority mapping: mapped into different queues based on priorities	System default is adopted in this example.
Management channel data plan		
Management VLAN and management IP address on the OLT side	Management VLAN ID: 8 Management VLAN type: smart VLAN Inband management IP address: 192.168.50.1/24	To configure the MDU from the OLT by logging in to the MDU, the management VLAN of the OLT and that of the MDU must be the same, and the management IP address of the OLT and that of the MDU must be in the same network segment.

Copyright © Huawei Technologies Co., Ltd.

Item	Data	Memo
Management VLAN and management IP address on the ONU side	Management VLAN ID: 8 Management VLAN type: smart VLAN Inband management IP address: 192.168.50.2/24	
Service channel data plan		
Internet access service	OLT VLAN ID: ● CVLAN ID: 256 x GPON port ID + 32 x Split ratio x (Splitter port ID - 1) + ONU port ID + 1 ● SVLAN: VLAN ID 100 and attribute stacking Upstream VLANs of the ONU: 1001-1016 Service flow ID: 101	Assume that the split ratio of the optical splitter is 1:32, the ONU is connected to port 1 on the optical splitter using the optical cable, and the user PC is connected to port 1 on the ONU. In this case, the inner VLAN is 258 according to the formula for calculating the inner VLAN. For details about the data plan, see **19.3.2 Data Planning**.
VoIP service	OLT VLAN ID (VLAN transparently transmitting the ONU service): 200 ONU VLAN ID: 200 Service flow ID: 201	For details about the data plan, see **19.3.2 Data Planning**.
Security data plan		
System security	Anti-DOS attack: disabled Anti-ICMP attack: disabled Anti-IP attack: disabled	System default is adopted in this example.
User security	Anti-MAC duplicate: disabled Anti-IP sproofing: disabled	System default is adopted in this example.
Service security	Forward the packet with PITP tag: enabled Forward the packet with DHCPv4 Option82: enabled Forward the packet with DHCPv6 Option18/37: enabled	In this example, the location information is added to packets by the ONU equipment and these packets are forwarded by the OLT equipment.

Copyright © Huawei Technologies Co., Ltd.

Data plan of the ONU side

Item	Data	Memo
HSI service data plan		
Port	Upstream port: 0/0/1 Service port: 0/3/1	-
Service VLAN	VLAN ID: 1001-1016 VLAN type: smart VLAN VLAN attribute: common	The ONU supporting 16 FE ports is used as an example. In actual configuration, plan the data according to actual capabilities of devices. For details about the data plan, see **19.3.2 Data Planning**.
Traffic profile	Profile ID: 8 Committed rate: 4 Mbit/s Priority: 0	For details about the data plan, see **19.3.2 Data Planning**.
Queue scheduling data plan		
Queue scheduling	Queue scheduling: strict priority (SQ) mode Priority mapping: mapped into different queues based on priorities	System default is adopted in this example.
Service security data plan		
System security	Anti-DOS attack: disabled Anti-ICMP attack: disabled Anti-IP attack: disabled	System default is adopted in this example.
User security	Anti-MAC duplicate: disabled Anti-IP sproofing: disabled	System default is adopted in this example.
PPPoE Service security	RAIO Type: PITP P RAIO Mode: common	PITP is recommended for PPPoE.
IPv4oE Service security	RAIO Type: DHCP Option 82 RAIO Mode: common	DHCPv4 option and DHCPv6 option are recommended for IPoE.
IPv6oE Service security	RAIO Type: DHCPv6 Option RAIO Mode: common	
Voice service data plan		

Copyright © Huawei Technologies Co., Ltd.

Item	Data	Memo
Media and signaling upstream VLANs	200	H.248 protocol is adopted in this example.
Media and signaling upstream port	0/0/1	
Media IP address and signaling IP address	11.11.11.11/24	
Default gateway IP address	11.11.11.11/24	
MG interface ID	0	
Signaling port ID	2944	
IP address of the primary MGC	200.200.200.200/24	
Port ID of the primary MGC	2944	
Coding	Text	
Transmission mode	UDP	
H248 version that MG starts to negotiate	1 (the negotiation starts from V1)	
Phone number	83110001-83110024	
Terminal identification	Terminal layering is not supported and the terminal identification ranges from 0 to 23.	
User priority	Cat2 for phone 1 Cat3 for phone 2 to phone 24 (default)	
User type	Common user (DEL user by default)	
System parameter	Default value	
Overseas parameter	Default value	
PSTN port attribute	Polarity-reversal	
Ringing current attribute	Default value	

Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Configure GPON ONU profiles.

1. Configure a DBA profile.

```
huawei(config)#dba-profile add profile-name fttb_dba type3 assure 8192 max
20480
```

2. Configure an ONU line profile.

```
huawei(config)#ont-lineprofile gpon profile-id 10 profile-name fttb(c)
huawei(config-gpon-lineprofile-10)#tcont 4 dba-profile-name fttb_dba
huawei(config-gpon-lineprofile-10)#gem add 11 eth tcont 4 cascade on
huawei(config-gpon-lineprofile-10)#gem add 12 eth tcont 4 cascade on
huawei(config-gpon-lineprofile-10)#gem add 13 eth tcont 4 cascade on
huawei(config-gpon-lineprofile-10)#gem mapping 11 0 vlan 8
huawei(config-gpon-lineprofile-10)#gem mapping 12 1 vlan 1001
huawei(config-gpon-lineprofile-10)#gem mapping 13 2 vlan 200
huawei(config-gpon-lineprofile-10)#commit
huawei(config-gpon-lineprofile-10)#quit
```

3. (Optional) Add an alarm profile.

   In this example, the default alarm profile is used and therefore the configuration of the alarm profile is not required.

Step 2 Add an ONU to an OLT.

Assume that the ID of GPON port 0/2/1 is 1, SN is 32303131B39FD641, management mode is SNMP, and the bound line profile is fttb(c). Connect the ONU to such a GPON port through the optical splitter.

There are two modes to add an ONT: add an ONT offline and confirm an automatically discovered ONU.

- Add an ONU offline.

```
huawei(config)#interface gpon 0/2
huawei(config-if-gpon-0/2)#ont add 1 ontid 1 sn-auth 32303131B39FD641
snmp ont-lineprofile-name fttb(c)
```

- Confirm an automatically discovered ONU.

```
huawei(config)#interface gpon 0/2
huawei(config-if-gpon-0/2)#port 1 ont-auto-find enable
huawei(config-if-gpon-0/2)#display ont autofind 1
huawei(config-if-gpon-0/2)#ont confirm 1 ontid 1 sn-auth 32303131B39FD641
snmp ont-lineprofile-name fttb(c)
```

1. (Optional) Bind the alarm profile to the ONU.

   In this example, default alarm profile 1 is used and therefore the configuration of the alarm profile is not required.

Step 3 Check the ONU status.

After an ONU is added, run the **display ont info** command to query the current status of the ONU. Ensure that **Config flag** of the ONU is **active**, **Run State** is **online**, and **Config state** is **normal**.

```
huawei(config-if-gpon-0/2)#display ont info 1 1
  ------------------------------------------------------------------------
  F/S/P                : 0/2/1
  ONT-ID               : 1
  Control flag         : active    //The ONU is activated.
  Run state            : online    //The ONU is online.
  Config state         : normal    //The ONU configurations are recovered
normally.
```


Copyright © Huawei Technologies Co., Ltd.

```
...//The rest of the response information is not provided here.
huawei(config-if-gpon-0/2)#quit
```

Step 4 Configure the inband management VLAN and IP address of the OLT.

```
huawei(config)#vlan 8 smart
huawei(config)#port vlan 8 0/19 0
huawei(config)#vlan priority 8 6
huawei(config)#interface vlanif 8
huawei(config-if-vlanif8)#ip address 192.168.50.1 24
huawei(config-if-vlanif8)#quit
```

Step 5 Configure the inband management VLAN and IP address of the ONU.

```
huawei(config)#interface gpon 0/2
huawei(config-if-gpon-0/2)#ont ipconfig 1 1 static ip-address 192.168.50.2 mask
255.255.255.0 gateway
192.168.50.1 vlan 8
huawei(config-if-gpon-0/2)#quit
```

Step 6 Configure an inband management service port.

```
huawei(config)#service-port 1 vlan 8 gpon 0/2/1 ont 1 gemport 11 multi-service
user-vlan 8 rx-cttr 6 tx-cttr 6
```

Step 7 Confirm that the management channel between the OLT and the ONU is available.

- On the OLT, run the **ping *192.168.50.2*** command to check the connectivity between the OLT and the ONU. The ICMP ECHO-REPLY packet from the ONU should be received.
- On the OLT, you can remote log in to the ONU to perform the configuration.

Step 8 Configure the channel for the Internet access service.

```
huawei(config)#vlan 100 smart
huawei(config)#vlan attrib 100 stacking
huawei(config)#port vlan 100 0/19 0
huawei(config)#service-port 101 vlan 100 gpon 0/2/1 ont 1 gemport 12 multi-
service
user-vlan 1001 tag-transform translate-and-add inner-vlan 258 rx-cttr 6 tx-cttr 6
```

Step 9 Configure the channel for the VoIP service.

```
huawei(config)#vlan 200 smart
huawei(config)#port vlan 200 0/19 0
huawei(config)#traffic table ip index 9 cir off priority 5 priority-policy local-
setting
huawei(config)#service-port 201 vlan 200 gpon 0/2/1 ont 1 gemport 13 multi-
service
user-vlan 200 rx-cttr 9 tx-cttr 9
```

Step 10 Configure LAG for upstream ports.

Configure upstream ports 0/19/0 and 0/19/1 into an aggregation group. Each member port in the aggregation group allocates packets based on the source MAC address. The working mode is LACP static aggregation.

```
huawei(config)#link-aggregation 0/19 0-1 ingress workmode lacp-static
```

Step 11 (Optional) When PPPoE is adopted, enable forwarding the packets with PITP tag on the OLT equipment.

```
huawei(config)#pitp permit-forwarding service-port 101 enable
```

Step 12 (Optional) When IPoE is adopted, enable forwarding the packets with DHCP option on the OLT equipment.

```
huawei(config)#dhcp-option82 permit-forwarding service-port 101 enable  //For IPv4
packets
huawei(config)#dhcpv6-option permit-forwarding port 0/2/1 ontid 1 enable  //For
IPv6 packets
```


Copyright © Huawei Technologies Co., Ltd.

Step 13 Save the configuration data on the OLT.

```
huawei(config)#save
```

Step 14 Log in to and configure the ONU.

You can remote log in to the ONU from the OLT to perform the configuration. By default, the user name is **root** and the password is **mduadmin**.

NOTE

The following steps are configured on the ONU side.

Step 15 Configuration the HSI service on the ONU side.

NOTE

This example creates one service port as an example. Each service port maps a user. When configuring another service port, map the corresponding SVLAN.

```
huawei(config)#vlan 1001-1016 smart
huawei(config)#port vlan 1001-1016 0/0 1
huawei(config)#traffic table ip index 8 cir 4096 priority 0 priority-policy local-
Setting
huawei(config)#service-port 101 vlan 1001 eth 0/3/1 multi-service user-vlan
untagged rx-cttr 8 tx-cttr 8
```

Step 16 (Optional) Configure the PITP function for PPPoE.

```
huawei(config)#raio-mode common pitp-pmode
huawei(config)#pitp enable pmode
```

Step 17 (Optional) Configure the DHCP option function for IPoE.

```
huawei(config)#raio-mode common dhcp-option82      //For DHCPv4 packets
huawei(config)#dhcp option82 enable                      //For DHCPv4 packets
huawei(config)#raio-mode common dhcpv6-option            //For DHCPv6 packets
huawei(config)#dhcpv6 option enable                      //For DHCPv6 packets
```

Step 18 Configure the voice service.

```
huawei(config)#vlan 200 smart
huawei(config)#port vlan 200 0/0 1
huawei(config)#interface vlanif 200
huawei(config-if-vlanif200)#ip address 11.11.11.11 24
huawei(config-if-vlanif200)#quit
huawei(config)#voip
huawei(config-voip)#ip address media 11.11.11.11 11.11.11.11
huawei(config-voip)#ip address signaling 11.11.11.11
huawei(config-voip)#quit
huawei(config)#ip route-static 200.200.200.0 24 11.11.11.11
huawei(config)#interface h248 0
  Are you sure to add MG interface?(y/n)[n]:y
huawei(config-if-h248-0)#if-h248 attribute mgip 11.11.11.11 mgport
 2944 code text transfer udp primary-mgc-ip1 200.200.200.200 primary-mgc-port
 2944 mg-media-ip1 11.11.11.11 start-negotiate-version 1
huawei(config-if-h248-0)#reset coldstart
  Are you sure to reset MG interface?(y/n)[n]:y
huawei(config-if-h248-0)#quit
huawei(config)#esl user
huawei(config-esl-user)#mgpstnuser batadd 0/3/0 0/3/23 0 terminalid 0 telno
83110001
huawei(config-esl-user)#mgpstnuser modify 0/3/0 priority cat2
huawei(config-esl-user)#quit
huawei(config)#pstnport
huawei(config-pstnport)#pstnport attribute batset 0/3/0 0/3/23 reverse-pole-pulse
enable
huawei(config-pstnport)#quit
```

Step 19 Save the configuration on the ONU side.

Copyright © Huawei Technologies Co., Ltd.

```
huawei(config)#save
```

----End

19.4 Configuring IPv6 Services in the FTTB+HGW Scenario

This section describes the methods for configuring IPv6 services in the FTTB+HGW scenario.

19.4.1 Application Scenario

The FTTB+HGW networking includes two scenarios: The ONU provides the voice service in one scenario and the HGW provides the voice service in another scenario. After IPv6 is introduced to the network, the voice service still uses IPv4 so that these two voice scenarios do not change after IPv6 introduction.

FTTB+HGW Application Scenario

Figure 19-5 shows an FTTB+HGW network. The OLT is deployed at the CO and connects to the MAN by aggregation, and the ONU is deployed in the buildings or street fiber distribution terminals. Access interfaces are deployed on the HGW that connects to the ONU using LAN or xDSL upstream transmission (deployed in user houses). Together with upper layer devices, the FTTB+HGW network supports the HSI and IPTV services implemented by the schemes of the Huawei fixed broadband solution for IPv6: IPv4/IPv6 DS+NAT+PPPoE, IPv4/IPv6 DS+NAT +IPoE, and DS-Lite+PPPoE (for the HSI services) and IPv4/IPv6 DS+IPoE and IPv4/IPv6 DS +PPPoE (for the IPTV service).

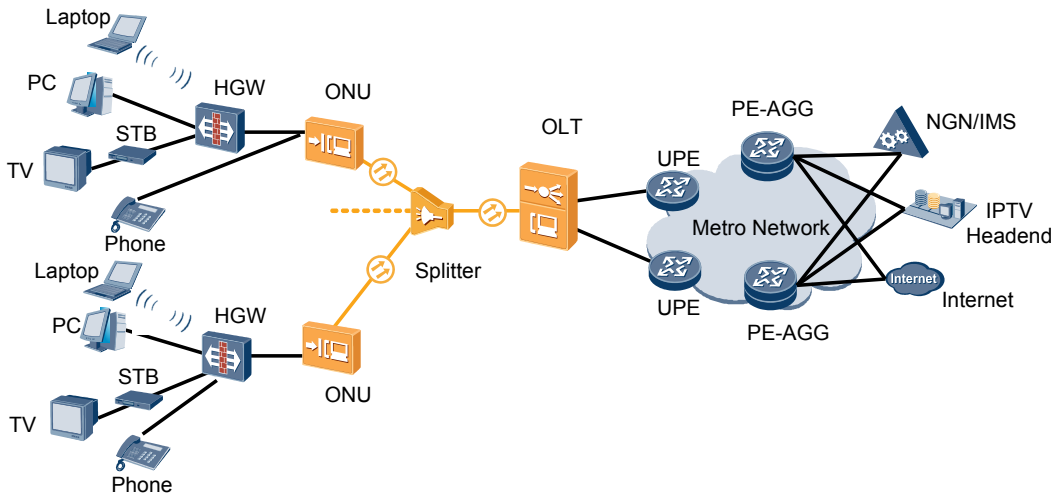
- Upstream networking: The HGW connects to the ONU through upstream ETH or xDSL port.
- HSI service: The HGW has Layer 3 functions (such as PPPoE dial-up and NAT), which enable multiple PCs of a family to access the Internet at the same time.
  - If the HGW uses the IPv4/IPv6 DS scheme, the PPPoE or IPoE channel that supports both IPv4 and IPv6 is established between the HGW and the BRAS. The OLT and ONU perform Layer 2 forwarding, irrespective of whether the access service is IPv4 or IPv6. Service configurations for IPv4 and IPv6 are the same. Only the ACL, anti-IP spoofing, and DHCP option configurations for IPv4 and IPv6 are different.
  - If the HGW uses the DS-Lite scheme, the PPPoE channel that supports only IPv6 is established between the HGW and the BRAS. As for IPv4, the HGW encapsulates IPv4 packets and transmits them to the BRAS or CGN using the 4in6 tunnel. The OLT and ONU perform Layer 2 forwarding, irrespective of whether the access service is IPv4 or IPv6. Service configurations for IPv4 and IPv6 are the same. Only the ACL, anti-IP spoofing, and DHCP option configurations for IPv4 and IPv6 are different.
- IPTV service: Users can preview or view IPTV programs by connecting an STB to the HGW. STB supports IPv4/IPv6 DS and uses IPv4 or IPv6 (cannot be used together) to carry IPTV services.
  - If the STB uses IPoE, choose the ONU preferentially to duplicate multicast flows. On the ONU, IPv6 and IPv4 multicast services are configured in the same way but with different commands. On the OLT, service channels to the ONU need to be established, multicast flows do not need to be duplicated, and IGMP IPv6 data needs to be configured.

Copyright © Huawei Technologies Co., Ltd.

- If the STB uses PPPoE, it establishes a PPPoE connection to the BRAS. The OLT, ONU, and HGW only forward PPPoE service flows and do not process multicast services. Therefore, this scheme is not recommended.

- Voice service: The voice service can be provided by the ONU with the build-in voice module or the build-in IAD of the HGW. The VoIP service on ONU or HGW is still implemented by IPv4.

Figure 19-5 FTTB+HGW service networking



19.4.2 Data Planning

This section describes the security, device management data, QoS, Internet service data, voice service data, and IPTV service data planning.

Security Planning

Security planning includes system security, user security, and service security, ensuring user services are provided properly from different dimensions.

In the FTTB+HGW networking scenario, only anti-IP spoofing and DHCP option of IPv6 and IPv4 services are different.

Anti-IP spoofing: This function needs to be configured separately for IPv6 services.

The anti-IP spoofing function can be enabled or disabled at three levels. This function takes effect only when it is enabled at all the three levels.

1. Global level: Run the **security anti-ipv6spoofing enable** command in global config mode.
2. VLAN level: Run the **security anti-ipv6spoofing enable** command in VLAN service profile mode.
3. Service port level: Run the **security anti-ipv6spoofing service-port** *serviceport-id* **enable** command.

DHCP option: The DHCP option for IPv4 is DHCPv4 option 82 and for IPv6 is DHCPv6 option 18/37.

Copyright © Huawei Technologies Co., Ltd.

The DHCPv6 option18 and option37 functions can be enabled or disabled at two levels. This function takes effect only when it is enabled at both levels.

1. Global level: Run the **dhcpv6 option enable** command in global config mode.
2. VLAN level: Run the **dhcpv6 option enable** command in VLAN service profile mode.

Device Management Data Planning

Device management data planning includes the management channel and IP address planning. The management channel for IPv6 and IPv4 services are the same.

Planning	Device or Service	Solution Introduction
Management channel	OLT	The device management uses single-tagged VLANs on the entire network.
	ONU	The device management uses single-tagged VLANs on the entire network.
	HGW	Single-tagged S-VLANs are used as management VLANs for all HGWs that need to be managed by the iTMS. The management VLANs for HGWs can be allocated to an entire network, an OLT, a PON board, or a PON port to identify services and physical locations. It is recommended that you set different HGW management VLANs for the OLTs connected to one SR to avoid an excessively large broadcast domain of the SR and convergence switch.
IP address planning	Device management	IPv4 private network IP addresses are still used as management IP addresses of the OLT and MDU devices.

Copyright © Huawei Technologies Co., Ltd.

Planning	Device or Service	Solution Introduction
	Internet	● IPv4 address: An HGW obtains the IPv4 address from the BRAS using PPPoE or DHCP. If IPoE dial-up is used, the static address can be configured. Meanwhile, as the DHCP server, the HGW allocates private network IP addresses to PCs. The NAT function enables these PCs to go online by sharing the IPv4 address allocated by the BRAS. – The BRAS can allocate a public network IP address to an HGW. – The BRAS can allocate a private network address to an HGW. The private network address is translated to the public network address by CGN (NAT44). ● IPv6 address: An HGW obtains the IPv6 address from the BRAS using PPPoE or DHCP. If IPoE dial-up is used, the static address can be configured. Meanwhile, the HGW as the DHCP server obtains the prefix of an IPv6 address, and allocates IPv6 addresses to connected PCs.
	IPTV service	● If the IPv4 protocol is used, an STB obtains the IP address from the BRAS using DHCP. ● If the IPv6 protocol is used, the STB obtains the IP address in either of the following ways: – Obtains the IP address from the BRAS using DHCPv6. – Obtains the IP address from the BRAS using SLAAC.
	VoIP service	The IPv4 protocol is still used. An ONU or HGW functions as the DHCP client to obtain the IP address using DHCP.
	TR069 service	The IPv4 protocol is still used. In scenarios in which TR069 is required for management maintenance and service provisioning, the HGW functions as the DHCP client to obtain a public network IP address from the DHCP server to connect the TR069 server ACS.

QoS Planning

The E2E QoS planning includes the flow classification, marking/scheduling policy, traffic monitoring, and DBA policy.

When the IPv6 protocol is used, the QoS planning is the same for both IPv6 and IPv4.

Copyright © Huawei Technologies Co., Ltd.

- Management service: IPv4
- Voice service: IPv4
- IPTV service: One user uses either IPv6 or IPv4 at one time. The QoS planning for IPv6 and IPv4 IPTV services is the same.
- Internet service: It is recommended that access devices use one flow to carry IPv6 and IPv4 Internet services. The QoS planning is the same for the flow that carries both IPv6 and IPv4 Internet services and the flow that carries only the IPv4 Internet service.

Internet Service Planning

The Internet service planning includes the VLAN and VLAN switching policy planning in different networking scenarios.

IPv6 and IPv4 Internet services: It is recommended that devices use one flow to carry IPv6 and IPv4 Internet services. This facilitates the control of the aggregate rate for IPv6 and IPv4 Internet services. The QoS planning is the same for the flow that carries both IPv6 and IPv4 Internet services and the flow that carries only the IPv4 Internet service.

Voice Service Data Planning

Voice service data planning includes the VLAN/VLAN switching policy planning in different networking scenarios, and voice protocol planning.

Even after IPv6 is used, the device still uses IPv4 to implement voice services.

IPTV Service Data Planning

IPTV service data planning includes the VLAN/VLAN switching policy planning in different networking scenarios, and IPTV service planning.

When the IPv6 protocol is used, one IPTV user uses either IPv6 or IPv4 at one time. The VLAN data planning for IPv6 is consistent with that for IPv4. For details, see **11.2.6 Principle of IPTV Service Data Plan**. The IPv6 version of the IGMP protocol is aslo known as multicast listener discovery (MLD). The following table lists the detailed data planning.

Data Item	Remarks
IGMP	The OLT and ONU use the IGMP IPv6 proxy.

Copyright © Huawei Technologies Co., Ltd.

Data Item	Remarks
IGMP version	The compatibility policies of the IGMP version on access devices are different on the network side (multicast router) and the user side (terminal). In normal application scenarios: 1. The device is usually the initiating party. The IGMP version on the multicast router can be seamlessly degraded without packet loss. 2. The terminal is usually the initiating party. The IGMP version on the device can be seamlessly degraded without packet loss. Recommended IGMP IPv6 protocol versions are as follows: ● When the network side is V1, the access device uses V1. ● When the network side is V2, the access device uses V1 or V2. ● When the network side is V1, the access device uses V1 or V2. ● When the network side is V2, the access device uses V2.
Multicast program	Static configuration is recommended. The OLT can also generate a multicast program library, that is, dynamically generate a program list according to the programs requested by users.
Multicasat preview profile	Not supported.
Multicast quick leave	The quick leave function is enabled (recommended) to help reduce the exchange of IGMP packets and save bandwidth resources.

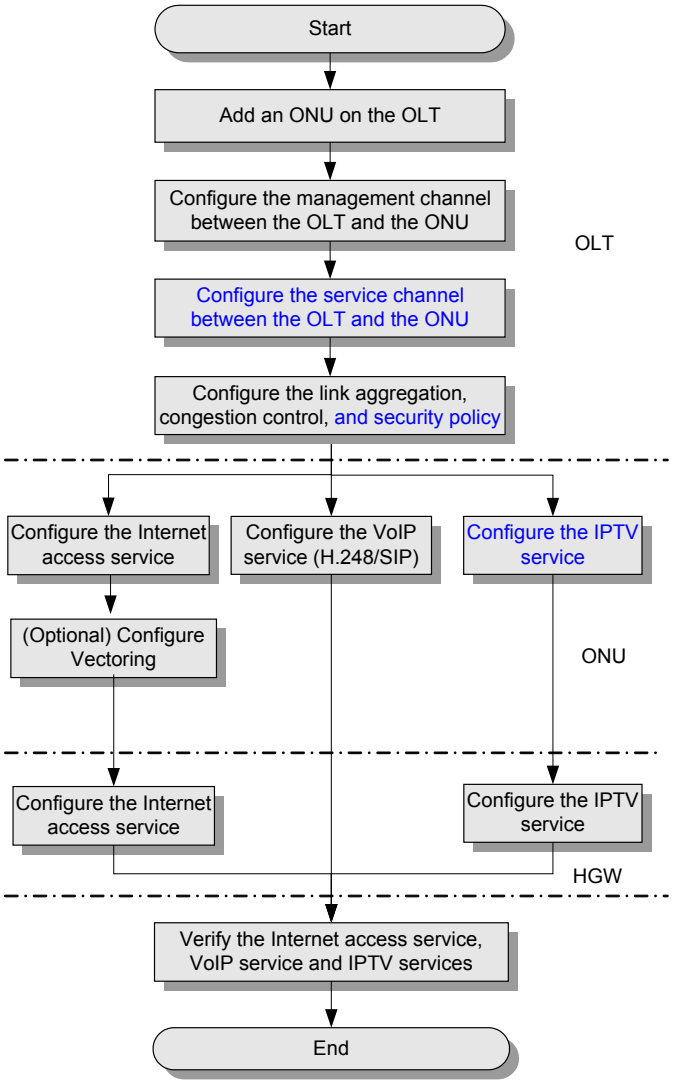
19.4.3 Configuration Procedure

This section describes IPv6 service configuration procedure by scenario, and compares it with the IPv4 service configuration procedure.

FTTB+HGW (ONU Provides the Voice Service) Configuration Procedure

The following figure shows the IPv6 service configuration procedure in the FTTB+HGW (ONU provides the voice service) scenario. In this scenario, the planning and configuration procedure/method for IPv6 and IPv4 services are almost the same except the following differences. On the OLT side, multicast service channels between the OLT and ONU and part configuration commands of the security policy are different. On the ONU side, configuration commands of IPTV multicast services are different. **19.2 Configuration Difference Between IPv6 and IPv4** shows the differences.

Copyright © Huawei Technologies Co., Ltd.



NOTE

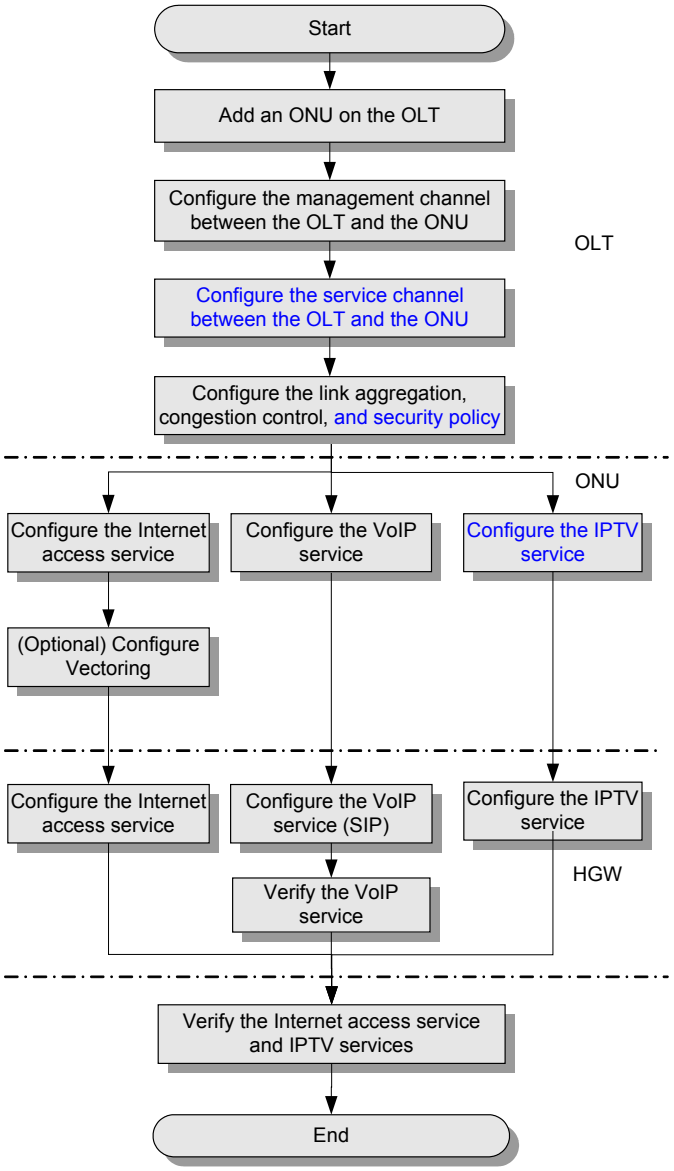
Texts in blue show the configuration (on OLT and ONU) difference between IPv6 and IPv4.

For differences between the HGW's IPv6 and IPv4 service processing, see documentation of the HGW products.

FTTB+HGW (HGW provides the voice service) Configuration Procedure

The following figure shows the IPv6 service configuration procedure in the FTTB+HGW (ONU provides the voice service) scenario. In this scenario, the planning and configuration procedure/ method for IPv6 and IPv4 services are almost the same except the following differences. On the OLT side: Multicast service channels between the OLT and ONU and part configuration commands of the safety policy are different. On the ONU side: Configuration commands of IPTV multicast services are different. **19.2 Configuration Difference Between IPv6 and IPv4** shows the differences.

Copyright © Huawei Technologies Co., Ltd.



NOTE

Texts in blue show the configuration (on OLT and ONU) difference between IPv6 and IPv4.

For differences between the HGW's IPv6 and IPv4 service processing, see documentation of the HGW products.

19.4.4 Configuration Example

Introduce the end-to-end service configuration based on the FTTB+HGW networking and the corresponding data plan.

Key Messages for Configuration

- Even after IPv6 is used, the voice service is still realized by IPv4.
- Even after IPv6 is used, the OLT and ONU implement Layer 2 forwarding for HSI service in this networking, irrespective of whether the access service is IPv4 or IPv6. Service configurations for IPv4 and IPv6 are the same. For the HSI service from one end user, one

Copyright © Huawei Technologies Co., Ltd.

service flow is used to carry IPv6 and IPv4 Internet services, and the same service VLAN is used.

- For multicast service, the ONU is the node to make multicast duplication. The configuration procedure is the same for IPv4 multicast and IPv6 multicase. The IPv4 multicast service and IPv6 multicast service can be configured in the same multicast VLAN on the ONU equipment.

Data plan on the OLT side

Item	Data	Memo
ONU data plan		
DBA profile	Profile name: fttb_dba Profile type: type3 Assured bandwidth: 8 Mbit/s Maximum bandwidth: 20 Mbit/s	The ONU is connected to OLT through the GPON interface.
Line profile	Profile name: fttb(c) Profile ID: 10 T-CONT ID: 4 GEM port ID for management service: 11 GEM port ID for Internet access service: 12 GEM port ID for VoIP service: 13	
Network topology data	PON port: 0/2/1 ONT ID: 1	
LAG data plan		
LAG	Ports: 0/19/0 and 0/19/1 Working mode: LACP static aggregation	Configure upstream ports 0/19/0 and 0/19/1 into an aggregation group. Each member port in the aggregation group allocates packets based on the source MAC address.
Queue scheduling data plan		
Queue scheduling	Queue scheduling: strict priority (SQ) mode Priority mapping: mapped into different queues based on priorities	System default is adopted in this example.
Management channel data plan		

Copyright © Huawei Technologies Co., Ltd.

Item	Data	Memo
Management VLAN and management IP address on the OLT side	Management VLAN ID: 8 Management VLAN type: smart VLAN Inband management IP address: 192.168.50.1/24	To configure the MDU from the OLT by logging in to the MDU, the management VLAN of the OLT and that of the MDU must be the same, and the management IP address of the OLT and that of the MDU must be in the same network segment.
Management VLAN and management IP address on the ONU side	Management VLAN ID: 8 Management VLAN type: smart VLAN Inband management IP address: 192.168.50.2/24	
Service channel data plan		
Internet access service	S-VLAN ID: 100; S-VLAN attribute: stacking C-VLAN ID: 1000-1016 Traffic profile: 6	Plan the Internet access service in per user per service per VLAN (PUPSPV) mode and apply S-VLAN+C-VLAN to differentiate users. The 802.1p priority of the Internet access service is 0, and rate limitation is not required. System traffic profile 6 can be used. For details, see **19.4.2 Data Planning**.
VoIP service	S-VLAN ID: 200 C-VLAN ID: 200 Traffic profile: 9	The voice over IP (VoIP) service is a carrier-operating, closed service and primarily adopts only S-VLAN tags, which are transparently transmitted by OLTs. The 802.1p priority of the VoIP service is 5, and rate limitation is not required. System traffic profiles do not meet the requirements and new traffic profile shall be configured. For details, see **19.4.2 Data Planning**.

Copyright © Huawei Technologies Co., Ltd.

Item	Data	Memo
VoD service	S-VLAN ID: 300 Traffic profile: 10	Plan the video on demand (VoD) service in per user per VLAN (PUPV) mode if possible, as the VoD service requires only a few VLAN resources. The VoD service is a carrier-operating, closed service and primarily adopts only S-VLAN tags, which are transparently transmitted by OLTs. The 802.1p priority of the VoD service is 4, and rate limitation is not required. System traffic profiles do not meet the requirements and new traffic profile shall be configured. For details, see **19.4.2 Data Planning**.
Multicast service	Multicast VLAN ID: 1000 Multicast cascading port: 0/2/1 IGMP version: IGMPv3 IGMP mode: IGMP proxy Multicast IP address range: 224.1.1.10-224.1.1.100 IP address of the multicast server: 10.10.10.10/24 Traffic profile: 10	The multicast service is a carrier-operating, closed service and primarily adopts only S-VLAN tags. Take the same traffic profile with the VoD service. For details, see **19.4.2 Data Planning**.
Security data plan		
System security	Anti-DOS attack: disabled Anti-ICMP attack: disabled Anti-IP attack: disabled	System default is adopted in this example.
User security	Anti-MAC duplicate: disabled Anti-IP sproofing: disabled	System default is adopted in this example.
Service security	Forward the packet with PITP tag: enabled Forward the packet with DHCPv4 Option82: enabled Forward the packet with DHCPv6 Option18/37: enabled	In this example, the location information is added to packets by the ONU equipment and these packets are forwarded by the OLT equipment.

Copyright © Huawei Technologies Co., Ltd.

Data plan of the ONU side

Item	Data	Memo
HSI service data plan		
Traffic profile	ID: 8 CIR: 4 Mbit/s VLAN priority: 0 Downstream priority policy: local-setting	-
User VLAN	Untagged	HGWs can send untagged packets or packets with user VLAN tags.
	User VLAN ID: 1, 2, 3...	
Queue scheduling data plan		
Queue scheduling	Queue scheduling: strict priority (SQ) mode Priority mapping: mapped into different queues based on priorities	System default is adopted in this example.
Service security data plan		
System security	Anti-DOS attack: disabled Anti-ICMP attack: disabled Anti-IP attack: disabled	System default is adopted in this example.
User security	Anti-MAC duplicate: disabled Anti-IP sproofing: disabled	System default is adopted in this example.
PPPoE Service security	RAIO Type: PITP P RAIO Mode: common	PITP is recommended for PPPoE.
IPv4oE Service security	RAIO Type: DHCP Option 82 RAIO Mode: common	DHCPv4 option and DHCPv6 option are recommended for IPoE.
IPv6oE Service security	RAIO Type: DHCPv6 Option RAIO Mode: common	
Voice service data plan		
Media and signaling upstream VLANs	200	H.248 protocol is adopted in this example.
Media and signaling upstream port	0/0/1	

Copyright © Huawei Technologies Co., Ltd.

Item	Data	Memo
Media IP address and signaling IP address	11.11.11.11/24	
Default gateway IP address	11.11.11.11/24	
MG interface ID	0	
Signaling port ID	2944	
IP address of the primary MGC	200.200.200.200/24	
Port ID of the primary MGC	2944	
Coding	Text	
Transmission mode	UDP	
H248 version that MG starts to negotiate	1 (the negotiation starts from V1)	
Phone number	83110001-83110024	
Terminal identification	Terminal layering is not supported and the terminal identification ranges from 0 to 23.	
User priority	Cat2 for phone 1 Cat3 for phone 2 to phone 24 (default)	
User type	Common user (DEL user by default)	
System parameter	Default value	
Overseas parameter	Default value	
PSTN port attribute	Polarity-reversal	
Ringing current attribute	Default value	
IPTV service data plan		

Copyright © Huawei Technologies Co., Ltd.

Item	Data	Memo
Traffic profile	ID: 10 CIR: off VLAN priority: 4 Downstream priority policy: local-setting	-
User VLAN in the scenario in which HGWs are upstream connected to an ONU through LANs	User VLAN ID: 1, 2, 3...	HGWs can send untagged packets or packets with user VLAN tags.
VPI/VCI of ADSL2 + users in the scenario in which HGWs are connected upstream to an ONU in ADSL2+ mode	VPI: 0 VCI: 35	Internet service providers (ISPs) provide VPI/VCI information.
VDSL2 path mode in the scenario in which HGWs are connected upstream to an ONU in VDSL2 mode	PTM	Both the central office and HGWs must support the PTM mode.
VLAN ID of the VoD service	300	The VoD service is a carrier-operating, closed service and primarily adopts only SVLAN tags, which are transparently transmitted by OLTs.
Multicast VLAN ID of the ONU	1000	-
Multicast VLAN ID of HGWs	43	A carrier generally specifies a globally unique multicast VLAN ID for HGWs.

Procedure

Step 1 Configure GPON ONU profiles.

1. Configure a DBA profile.

```
huawei(config)#dba-profile add profile-name fttb_dba type3 assure 8192 max 20480
```

2. Configure an ONU line profile.

```
huawei(config)#ont-lineprofile gpon profile-id 10 profile-name fttb(c)
huawei(config-gpon-lineprofile-10)#tcont 4 dba-profile-name fttb_dba
```


Copyright © Huawei Technologies Co., Ltd.

```
huawei(config-gpon-lineprofile-10)#gem add 11 eth tcont 4 cascade on
huawei(config-gpon-lineprofile-10)#gem add 12 eth tcont 4 cascade on
huawei(config-gpon-lineprofile-10)#gem add 13 eth tcont 4 cascade on
huawei(config-gpon-lineprofile-10)#gem mapping 11 0 vlan 8
huawei(config-gpon-lineprofile-10)#gem mapping 12 1 vlan 1001
huawei(config-gpon-lineprofile-10)#gem mapping 13 2 vlan 200
huawei(config-gpon-lineprofile-10)#commit
huawei(config-gpon-lineprofile-10)#quit
```

3. (Optional) Add an alarm profile.

   In this example, the default alarm profile is used and therefore the configuration of the alarm profile is not required.

Step 2 Add an ONU to an OLT.

Assume that the ID of GPON port 0/2/1 is 1, SN is 32303131B39FD641, management mode is SNMP, and the bound line profile is fttb(c). Connect the ONU to such a GPON port through the optical splitter.

There are two modes to add an ONT: add an ONT offline and confirm an automatically discovered ONU.

- Add an ONU offline.

```
huawei(config)#interface gpon 0/2
huawei(config-if-gpon-0/2)#ont add 1 ontid 1 sn-auth 32303131B39FD641
snmp ont-lineprofile-name fttb(c)
```

- Confirm an automatically discovered ONU.

```
huawei(config)#interface gpon 0/2
huawei(config-if-gpon-0/2)#port 1 ont-auto-find enable
huawei(config-if-gpon-0/2)#display ont autofind 1
huawei(config-if-gpon-0/2)#ont confirm 1 ontid 1 sn-auth 32303131B39FD641
snmp ont-lineprofile-name fttb(c)
```

1. (Optional) Bind the alarm profile to the ONU.

   In this example, default alarm profile 1 is used and therefore the configuration of the alarm profile is not required.

Step 3 Check the ONU status.

After an ONU is added, run the **display ont info** command to query the current status of the ONU. Ensure that **Config flag** of the ONU is **active**, **Run State** is **online**, and **Config state** is **normal**.

```
huawei(config-if-gpon-0/2)#display ont info 1 1
  ------------------------------------------------------------------------
  F/S/P                : 0/2/1
  ONT-ID               : 1
  Control flag         : active    //The ONU is activated.
  Run state            : online    //The ONU is online.
  Config state         : normal    //The ONU configurations are recovered
normally.
...//The rest of the response information is not provided here.
huawei(config-if-gpon-0/2)#quit
```

Step 4 Configure the inband management VLAN and IP address of the OLT.

```
huawei(config)#vlan 8 smart
huawei(config)#port vlan 8 0/19 0
huawei(config)#vlan priority 8 6
huawei(config)#interface vlanif 8
huawei(config-if-vlanif8)#ip address 192.168.50.1 24
huawei(config-if-vlanif8)#quit
```


Copyright © Huawei Technologies Co., Ltd.

Step 5 Configure the inband management VLAN and IP address of the ONU.

```
huawei(config)#interface gpon 0/2
huawei(config-if-gpon-0/2)#ont ipconfig 1 1 static ip-address 192.168.50.2 mask
255.255.255.0 gateway
192.168.50.1 vlan 8
huawei(config-if-gpon-0/2)#quit
```

Step 6 Configure an inband management service port.

```
huawei(config)#service-port 1 vlan 8 gpon 0/2/1 ont 1 gemport 11 multi-service
user-vlan 8 rx-cttr 6 tx-cttr 6
```

Step 7 Confirm that the management channel between the OLT and the ONU is available.

- On the OLT, run the **ping *192.168.50.2*** command to check the connectivity between the OLT and the ONU. The ICMP ECHO-REPLY packet from the ONU should be received.
- On the OLT, you can remote log in to the ONU to perform the configuration.

Step 8 Configure a channel for the Internet access service.

```
huawei(config)#vlan 100 smart
huawei(config)#vlan attrib 100 stacking
huawei(config)#port vlan 100 0/19 0
huawei(config)#service-port vlan 100 gpon 0/2/1 ont 1 gemport 12 multi-service
user-vlan 1001 tag-transform translate-and-add rx-cttr 6 tx-cttr 6
```

Step 9 Configure a channel for the Voice service.

```
huawei(config)#vlan 200 smart
huawei(config)#port vlan 200 0/19 0
huawei(config)#traffic table ip index 9 cir off priority 5 priority-policy local-
setting
huawei(config)#service-port vlan 200 gpon 0/2/1 ont 1 gemport 13 multi-service
user-vlan 200 rx-cttr 9 tx-cttr 9
```

Step 10 Configure a channel for the VoD service.

```
huawei(config)#vlan 300 smart
huawei(config)#port vlan 300 0/19 0
huawei(config)#traffic table ip index 10 cir off priority 4 priority-policy local-
Setting
huawei(config)#service-port vlan 300 gpon 0/2/1 ont 1 gemport 14 multi-service
user-vlan 300 rx-cttr 10 tx-cttr 10
```

Step 11 Configure a channel for the multicast service.

```
huawei(config)#vlan 1000 smart
huawei(config)#port vlan 1000 0/19 0
huawei(config)#service-port vlan 1000 gpon 0/2/1 ont 1 gemport 14 multi-service
user-vlan 1000 rx-cttr 10 tx-cttr 10
huawei(config)#btv
huawei(config-btv)#igmp cascade-port 0/2/1 ontid 1 gemport-index 14
huawei(config)#multicast-vlan 1000
huawei(config-mvlan1000)#igmp ipv6 version v2
huawei(config-mvlan1000)#igmp ipv6 mode proxy
  Are you sure to change IGMP IPv6 mode?(y/n)[n]:y
huawei(config-mvlan1000)#igmp uplink-port 0/19/0
huawei(config-mvlan1000)#igmp program add batch ipv6 ff15:: to-ipv6 ff15::ffff
 source-ipv6 2000::1
```

Step 12 Configure LAG for upstream ports.

Configure upstream ports 0/19/0 and 0/19/1 into an aggregation group. Each member port in the aggregation group allocates packets based on the source MAC address. The working mode is LACP static aggregation.

```
huawei(config)#link-aggregation 0/19 0-1 ingress workmode lacp-static
```

Step 13 (Optional) When PPPoE is adopted, enable forwarding the packets with PITP tag on the OLT equipment.

Copyright © Huawei Technologies Co., Ltd.

```
huawei(config)#pitp permit-forwarding service-port 101 enable
```

Step 14 (Optional) When IPoE is adopted, enable forwarding the packets with DHCP option on the OLT equipment.

```
huawei(config)#dhcp-option82 permit-forwarding service-port 101 enable   //For IPv4
packets
huawei(config)#dhcpv6-option permit-forwarding port 0/2/1 ontid 1 enable   //For
IPv6 packets
```

Step 15 Save the configuration data on the OLT.

```
huawei(config)#save
```

Step 16 Log in to and configure the ONU.

You can remote log in to the ONU from the OLT to perform the configuration. By default, the user name is **root** and the password is **mduadmin**.

NOTE

The following steps are configured on the ONU side.

Step 17 Configuration the HSI service on the ONU side.

NOTE

This example creates one service port as an example. Each service port maps a user. When configuring another service port, map the corresponding SVLAN.

```
huawei(config)#vlan 1001-1016 smart
huawei(config)#port vlan 1001-1016 0/0 1
huawei(config)#traffic table ip index 8 cir 4096 priority 0 priority-policy local-
setting
```

Configurations for untagged packets and packets with user VLAN tags are different.

- For untagged packets, the configuration is as follows (assuming that the VLAN ID is 1001):
  //Create service port 101, bind port 0/3/1 to it, set the user VLAN to untagged, and bind traffic profile 8 to the user VLAN./ huawei(config)#**service-port 101 vlan 1001 eth 0/3/1 multi-service user-vlan untagged rx-cttr 8 tx-cttr 8**
- For packets with user VLAN tags, the configuration is as follows (assuming that the user VLAN ID is 10 and the VLAN ID is 1001):
  //Create service port 101, bind port 0/3/1 to it, set the user VLAN ID to 10, and bind traffic profile 8 to the user VLAN./ huawei(config)#**service-port 101 vlan 1001 eth 0/3/1 multi-service user-vlan 10 rx-cttr 8 tx-cttr 8**

Step 18 (Optional) Configure the PITP function for PPPoE.

```
huawei(config)#raio-mode common pitp-pmode
huawei(config)#pitp enable pmode
```

Step 19 (Optional) Configure the DHCP option function for IPoE.

```
huawei(config)#raio-mode common dhcp-option82      //For DHCPv4 packets
huawei(config)#dhcp option82 enable                      //For DHCPv4 packets
huawei(config)#raio-mode common dhcpv6-option            //For DHCPv6 packets
huawei(config)#dhcpv6 option enable                      //For DHCPv6 packets
```

Step 20 Configure the voice service.

```
huawei(config)#vlan 200 smart
huawei(config)#port vlan 200 0/0 1
huawei(config)#interface vlanif 200
huawei(config-if-vlanif200)#ip address 11.11.11.11 24
huawei(config-if-vlanif200)#quit
huawei(config)#voip
huawei(config-voip)#ip address media 11.11.11.11 11.11.11.11
```


Copyright © Huawei Technologies Co., Ltd.

```
huawei(config-voip)#ip address signaling 11.11.11.11
huawei(config-voip)#quit
huawei(config)#ip route-static 200.200.200.0 24 11.11.11.11
huawei(config)#interface h248 0
  Are you sure to add MG interface?(y/n)[n]:y
huawei(config-if-h248-0)#if-h248 attribute mgip 11.11.11.11 mgport
 2944 code text transfer udp primary-mgc-ip1 200.200.200.200 primary-mgc-port
 2944 mg-media-ip1 11.11.11.11 start-negotiate-version 1
huawei(config-if-h248-0)#reset coldstart
  Are you sure to reset MG interface?(y/n)[n]:y
huawei(config-if-h248-0)#quit
huawei(config)#esl user
huawei(config-esl-user)#mgpstnuser batadd 0/3/0 0/3/23 0 terminalid 0 telno
83110001
huawei(config-esl-user)#mgpstnuser modify 0/3/0 priority cat2
huawei(config-esl-user)#quit
huawei(config)#pstnport
huawei(config-pstnport)#pstnport attribute batset 0/3/0 0/3/23 reverse-pole-pulse
enable
huawei(config-pstnport)#quit
```

Step 21 Configure the VoD service.

Create VLAN 300 with the common attribute and add upstream port 0/0/1 to the VLAN.

```
huawei(config)#vlan 300 smart huawei(config)#port vlan 300 0/0 1
```

Configure a traffic profile for the IPTV service.

The IEEE 802.1p priority of the IPTV service is 4, and rate limitation is not required. To check whether any existing traffic profile meets the requirements, run the **display traffic table ip** command. In this example, the query result shows that no traffic profile meets the requirements, so a traffic profile needs to be configured.

Add traffic profile 10 and set *priority-policy* to **local-setting**. Then, traffic is scheduled based on the priority specified in the traffic profile.

```
huawei(config)#traffic table ip index 10 cir off priority 4 priority-policy local-
setting
```

Configure a service flow for the VoD service.

Configurations vary according to upstream interface types of HGWs.

- If HGWs are connected to an ONU upstream through LANs and upstream packets contain user VLAN tags, the ONU needs to perform a switch between user VLAN IDs and SVLAN IDs.

  Assume that the user VLAN ID is 1 and the Ethernet port is 0/3/1. Add a service flow as follows:

  ```
  huawei(config)#service-port 301 vlan 300 eth 0/3/1 multi-service user-vlan 1 rx-
  cttr 10 tx-cttr 10
  ```

- If HGWs are connected to an ONU upstream in ADSL2+ mode, upstream packets contain users' PVC information so the ONU needs to perform a switch between PVC information and SVLAN IDs.

  Assume that the VPI/VCI is 0/35 and the ADSL2+ port is 0/2/0. Add a service flow as follows:

  ```
  huawei(config)#service-port 301 vlan 300 adsl vpi 0 vci 35 0/2/0 multi-service
  user-vlan untagged rx-cttr 10 tx-cttr 10
  ```

- If HGWs are connected to an ONU upstream in VDSL2 mode, formats of upstream packets depend on the encapsulation mode.

Copyright © Huawei Technologies Co., Ltd.

Assume that the VDSL2 path mode is PTM mode, port is 0/1/0, and packets from the user VLAN are untagged. Add a service flow as follows:

```
huawei(config)#service-port 301 vlan 300 vdsl mode ptm 0/1/0 multi-service user-vlan untagged rx-cttr 10 tx-cttr 10
```

Step 22 Configure the multicast service.

```
huawei(config)#vlan 1000 smart
huawei(config)#port vlan 1000 0/0 1
huawei(config)#multicast-vlan 1000
huawei(config-mvlan1000)#igmp ipv6 version v2
huawei(config-mvlan1000)#igmp ipv6 mode proxy
  Are you sure to change IGMP IPv6 mode?(y/n)[n]:y
huawei(config-mvlan1000)#igmp uplink-port 0/0/1
huawei(config-mvlan1000)#igmp program add batch ipv6 ff15:: to-ipv6 ff15::ffff
 source-ipv6 2000::1
huawei(config-mvlan1000)#quit
```

Configure a service flow for the multicast service.

Configurations vary according to upstream interface types of HGWs.

- If HGWs are connected to an ONU upstream through LANs, assume that the user VLAN ID is 43 and the Ethernet port is 0/3/1, and add a service flow as follows:
  ```
  huawei(config)#service-port 401 vlan 1000 eth 0/3/1 multi-service user-vlan 43 rx-cttr 10 tx-cttr 10
  ```
- If HGWs are connected to an ONU upstream in ADSL2+ mode, assume that the VPI/VCI is 0/35 and the ADSL2+ port is 0/2/0, and add a service flow as follows:
  ```
  huawei(config)#service-port 401 vlan 1000 adsl vpi 0 vci 35 0/2/0 multi-service user-vlan untagged rx-cttr 10 tx-cttr 10
  ```
- If HGWs are connected to an ONU upstream in VDSL2 mode, assume that the VDSL2 path mode is PTM mode, the user VLAN ID is 43, and the VDSL2 port is 0/1/0, and add a service flow as follows:
  ```
  huawei(config)#service-port 401 vlan 1000 vdsl mode ptm 0/1/0 multi-service user-vlan 43 rx-cttr 10 tx-cttr 10
  ```

```
huawei(config-mvlan1000)#btv
huawei(config-btv)#igmp user add service-port 401 no-auth
huawei(config-btv)#multicast-vlan 1000
huawei(config-mvlan1000)#igmp multicast-vlan member service-port 401
huawei(config-mvlan1000)#quit
```

Step 23 Save the configuration on the ONU side.

```
huawei(config)#save
```

----End

19.5 Configuring IPv6 Services in the FTTH (Bridging ONT) Scenario

This section describes the methods for configuring IPv6 services in the FTTH (bridging ONT) scenario.

19.5.1 Application Scenarios

The FTTH (bridging ONT) supports multiple IPv6 HSI and IPTV service schemes.

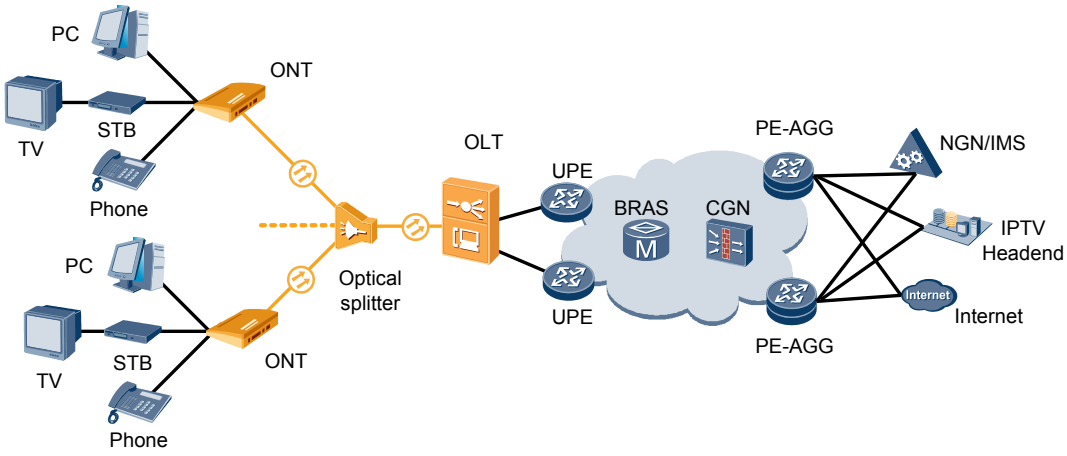
Copyright © Huawei Technologies Co., Ltd.

FTTH (Bridging ONT) Application Scenario

As shown in **Figure 19-6**, the FTTH (bridging ONT) works with upper-layer devices to support DS+NAT+PPPoE/DS+NAT+IPoE HSI and DS+IPoE or DS+PPPoE IPTV services in the Huawei fixed network IPv6 solution.

- For the voice service: An ONT with a bulit-in voice module can directly provide VoIP services for users. The ONT still processes VoIP services using IPv4.
- Internet service: The PC and BRAS support the IPv4/IPv6 dual-stack, and can be connected through the PPPoE or IPoE dial-up. The OLT and ONT perform Layer 2 forwarding for both IPv4 and IPv6 user services, which can be configured almost in the same way. The only difference is that commands for configuring the ACL and security (DHCP option and anti-IP spoofing) features are different.
- IPTV service: STBs support IPv4/IPv6 dual-stack and carry IPTV services using either IPv4 or IPv6.
  - When STBs use IPoE and the OLT functions as the multicast duplication point, the process for configuring IPv6 and IPv4 multicast services is the same, but commands are different. The ONTs perform Layer 2 forwarding for only IPTV services, and the configurations for IPv6 and IPv4 multicast services are the same on the ONT side.
  - When STBs use the PPPoE dial-up, they directly connect to the BRAS by PPPoE. The OLT and ONTs only forward PPPoE services instead of processing multicast services. This solution is not recommended.

Figure 19-6 FTTH (bridging ONT) service networking



19.5.2 Data Planning

This section describes the security, device management data, QoS, Internet service data, voice service data, and IPTV service data planning.

Security Planning

Security planning includes system security, user security, and service security, ensuring user services are provided properly from different dimensions.

In the FTTH (briding ONT) networking scenario, only anti-IP spoofing and DHCP option of IPv6 and IPv4 services are different.

Copyright © Huawei Technologies Co., Ltd.

Anti-IP spoofing: This function needs to be configured separately for IPv6 services.

The anti-IP spoofing function can be enabled or disabled at three levels. This function takes effect only when it is enabled at all the three levels.

1. Global level: Run the **security anti-ipv6spoofing enable** command in global config mode.
2. VLAN level: Run the **security anti-ipv6spoofing enable** command in VLAN service profile mode.
3. Service port level: Run the **security anti-ipv6spoofing service-port** *serviceport-id* **enable** command.

DHCP option: The DHCP option for IPv4 is DHCPv4 option 82 and for IPv6 is DHCPv6 option 18/37.

The DHCPv6 option18 and option37 functions can be enabled or disabled at two levels. This function takes effect only when it is enabled at both levels.

1. Global level: Run the **dhcpv6 option enable** command in global config mode.
2. VLAN level: Run the **dhcpv6 option enable** command in VLAN service profile mode.

Device Management Data Planning

Device management data planning includes the management channel and IP address planning. The management channel for IPv6 and IPv4 services is the same.

Planning	Device or Service	Solution Introduction
Management channel	OLT	The device management uses single-tagged VLANs on the entire network.

Copyright © Huawei Technologies Co., Ltd.

Planning	Device or Service	Solution Introduction
IP address planning (bridging ONT)	Internet	● IPv4 address: The PC obtains the IPv4 address from the BRAS using PPPoE or IPoE. – The BRAS can allocate a public network IP address to the PC. – The BRAS can allocate a private network address to the PC. The private address is translated to the public network address by CGN (NAT44). – When the IPoE dial-up is used, the static IPv4 address can be allocated to the PC. ● IPv6 address: The PC obtains the IPv4 address from the BRAS using PPPoE or IPoE. – The PC can also obtain the IP address from the BRAS using DHCPv6. – The PC can aslo obtain the IP address from the BRAS using SLAAC. – When the IPoE dial-up is used, the static IPv4 address can be allocated to the PC. In all above-mentioned situations, the ONT is only used for transparent transmission, but does not participate in the address allocation.
	IPTV service	● If the IPv4 protocol is used, an STB obtains the IP address from the BRAS using DHCP. ● If the IPv6 protocol is used, the STB obtains the IP address in either of the following ways: – Obtains the IP address from the BRAS using DHCPv6. – Obtains the IP address from the BRAS using SLAAC. In all above-mentioned situations, the ONT is only used for transparent transmission, but does not participate in the address allocation.
	VoIP service	The IPv4 protocol is still used. The ONT functions as the DHCP client to obtain an IP address from the DHCP server, or the NMS issues a static IP address to the ONT using the configuration file. Voice media/signaling flows at multiple POTS ports share one IP address. Media flows are differentiated by port.

Copyright © Huawei Technologies Co., Ltd.

QoS Planning

The E2E QoS planning includes the flow classification, marking/scheduling policy, traffic monitoring, and DBA policy.

When the IPv6 protocol is used, the QoS planning is the same for both IPv6 and IPv4.

- Management service: IPv4
- Voice service: IPv4
- IPTV service: One user uses either IPv6 or IPv4 at one time. The QoS planning for IPv6 and IPv4 IPTV services is the same.
- Internet service: It is recommended that devices use one flow to carry IPv6 and IPv4 Internet services. The QoS planning is the same for the flow that carries both IPv6 and IPv4 Internet services and the flow that carries only the IPv4 Internet service.

Internet Service Planning

The Internet service planning includes the VLAN and VLAN switching policy planning in different networking scenarios.

IPv6 and IPv4 Internet services: It is recommended that devices use one flow to carry IPv6 and IPv4 Internet services. This facilitates the control of the aggregate rate for IPv6 and IPv4 Internet services. The QoS planning is the same for the flow that carries both IPv6 and IPv4 Internet services and the flow that carries only the IPv4 Internet service.

Voice Service Data Planning

Voice service data planning includes the VLAN/VLAN switching policy planning in different networking scenarios, and the voice protocol planning.

When the IPv6 protocol is used, the voice service still uses IPv4 to implement voice services.

IPTV Service Data Planning

IPTV service data planning includes the VLAN/VLAN switching policy planning in different networking scenarios, and IPTV service planning.

When the IPv6 protocol is used, one IPTV user uses either IPv6 or IPv4 at one time. The VLAN data planning for IPv6 is consistent with that for IPv4. For details, see **9.6.5 Principle of IPTV Service Data Plan**.

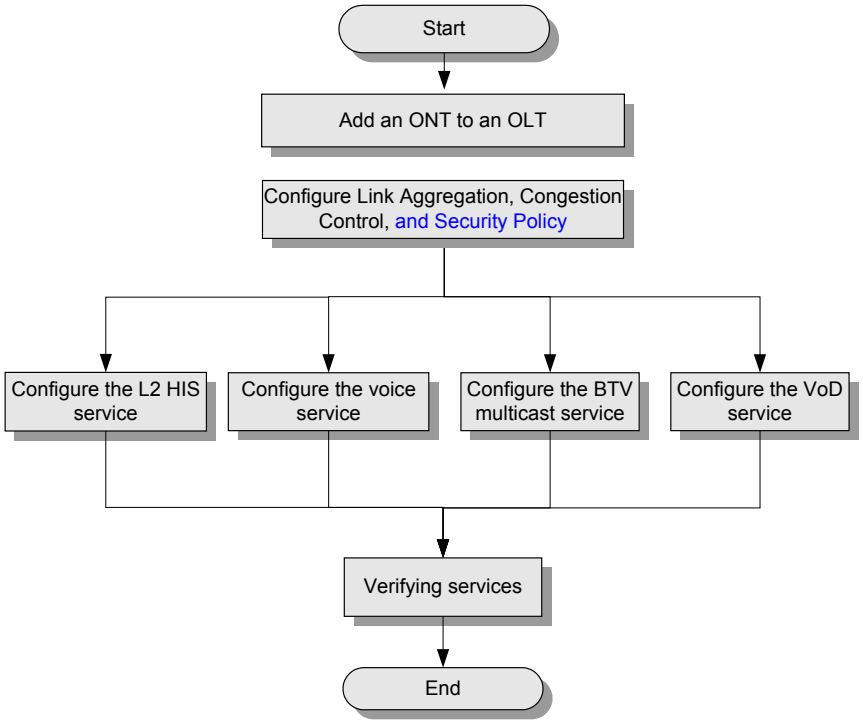
19.5.3 Configuration Procedure

This section describes IPv6 configuration procedure, and compares it with the IPv4 configuration procedure.

FTTH (Bridging ONT) Configuration Procedure

After IPv6 is introduced to the FTTH (bridging ONT) scenario, the service configuration procedure is shown in the following figure. When IPv6 is introduced, the configurations for security features and BTV multicast services on the OLT side are different from those of IPv4. Other configurations do not change. For differences, see **19.2 Configuration Difference Between IPv6 and IPv4**.

Copyright © Huawei Technologies Co., Ltd.



NOTE

Texts in blue show the configuration difference between IPv6 and IPv4.

19.5.4 Configuration Example

Introduce the end-to-end service configuration based on the FTTH (Bridging ONT) networking and the corresponding data plan.

Key Messages for Configuration

In this example, two ONTs are connected to the same PON port of the OLT. Triple play services are required

- Even after IPv6 is used, the voice service is still realized by IPv4.
- Even after IPv6 is used, the OLT and ONT implement Layer 2 forwarding for HSI service in this networking, irrespective of whether the access service is IPv4 or IPv6. Service configurations for IPv4 and IPv6 are the same. For the HSI service from one end user, one service flow is used to carry IPv6 and IPv4 Internet services, and the same service VLAN is used.
- For multicast service, the OLT is the node to make multicast duplication. The configuration procedure is the same for IPv4 multicast and IPv6 multicase. The IPv4 multicast service and IPv6 multicast service can be configured in the same multicast VLAN on the OLT equipment.

Data plan on the OLT side

The data of the bridging ONT can be configured through the web, the NMS, or the CLI at the OLT side. In this example, the data of the ONT is configured through the CLI at the OLT side.

Copyright © Huawei Technologies Co., Ltd.

Item	Data	Memo
ONT data plan		
DBA profile	Profile name: ftth_dba Profile type: type3 Assured bandwidth: 8 Mbit/s Maximum bandwidth: 20 Mbit/s	The ONTs are connected to the OLT through the GPON port.
ONT line profile	Profile name: ftth T-CONT ID: 4 GEM port ID for management services: 11 GEM port ID for voice services: 12 GEM port ID for video services: 13 GEM port ID for Internet access services: 14	
ONT service profile	Profile name: ftth ONT port capability set: adaptive	
Network topology data	PON port: 0/1/0 ONT IDs: 1 and 2	
LAG data plan		
LAG	Ports: 0/19/0 and 0/19/1 Working mode: LACP static aggregation	Configure upstream ports 0/19/0 and 0/19/1 into an aggregation group. Each member port in the aggregation group allocates packets based on the source MAC address.
Queue scheduling data plan		
Queue scheduling	Queue scheduling: strict priority (SQ) mode Priority mapping: mapped into different queues based on priorities	System default is adopted in this example.
Security data plan		
System security	Anti-DOS attack: disabled Anti-ICMP attack: disabled Anti-IP attack: disabled	System default is adopted in this example.

Copyright © Huawei Technologies Co., Ltd.

Item	Data	Memo
User security	Anti-MAC duplicate: disabled Anti-IP sproofing: disabled	System default is adopted in this example.
PPPoE Service security	RAIO Type: PITP P RAIO Mode: common	PITP is recommended for PPPoE.
IPv4oE Service security	RAIO Type: DHCP Option 82 RAIO Mode: common	DHCPv4 option and DHCPv6 option are recommended for IPoE.
IPv6oE Service security	RAIO Type: DHCPv6 Option RAIO Mode: common	
HSI service data plan		
ONT line profile	Profile name: ftth T-CONT ID: 4 GEM port ID for Internet access service: 14	For details, see **19.5.2 Data Planning**.
ONT service profile	Profile name: ftth ONT port capability set: adaptive	
Traffic profile	Profile name: ftth_hsi CIR: 4Mbit/s Priority: 0	
Network topology data	Upstream port: 0/19/0 PON port: 0/1/0 ONT IDs: 1 and 2 ID of the port on the ONT that is connected to the PC: 1	
Voice service data plan		
ONT line profile	Profile name: ftth T-CONT ID: 4 GEM port ID: 12	For details, see **19.5.2 Data Planning**.
ONT service profile	Profile name: ftth ONT port capability set: adaptive	

Copyright © Huawei Technologies Co., Ltd.

Item	Data	Memo
Traffic profile	Profile name: ftth_voip CIR: not limited Priority: 5	
Networking data	IP address of the MGC server: 200.200.200.200/24 Port ID of the MGC server: 2944	
BTV multicast service data plan		
ONT line profile	Profile name: ftth T-CONT ID: 4 GEM port ID: 13	For details, see **19.5.2 Data Planning**.
ONT service profile	Profile name: ftth ONT port capability set: adaptive	
Traffic profile	ID: 8 802.1p priority: 4 CIR: off (unlimited) Priority-based scheduling policy: local-setting	
VLAN Plan	SVLAN ID: 1000 VLAN type: smart VLAN attribute: common	
VLAN Translation Policy	ONT: duplicates packets based on user ports and multicast VLANs (MVLANs) are stripped off downstream. OLT: duplicates multicast packets based on PON ports with MVLAN unchanged.	
Multicast service data	Multicast protocol: IGMP proxy Multicast version: IGMPv2 Multicast program: dynamic obtaining mode Program address area: ff15::-ff15::ffff	
VOD service data plan		

Copyright © Huawei Technologies Co., Ltd.

Item	Data	Memo
ONT line profile	Profile name: ftth T-CONT ID: 4 GEM port ID: 13	For details, see **19.5.2 Data Planning**.
ONT service profile	Profile name: ftth ONT port capability set: adaptive	
Traffic profile	ID: 8 802.1p priority: 4 CIR: off (unlimited) Priority-based scheduling policy: local-setting	
VLAN Plan	● SVLAN ID: 1100 ● VLAN type: smart ● VLAN attribute: common ● CVLAN=SVLAN	
VLAN Translation Policy	ONT: adds CVLAN tags to iTV service packets. OLT: transparently transmits packets with SVLANs.	

Procedure

Step 1 Configure LAG for upstream ports.

Configure upstream ports 0/19/0 and 0/19/1 into an aggregation group. Each member port in the aggregation group allocates packets based on the source MAC address. The working mode is LACP static aggregation.

```
huawei(config)#link-aggregation 0/19 0-1 ingress workmode lacp-static
```

Step 2 Configure GPON ONT profiles.

1. Configure a DBA profile.

   Create the same DBA profile for different types of services. Set the profile name to **ftth_dba**, profile type to **type3**, assured bandwidth to 8 Mbit/s, and maximum bandwidth to 20 Mbit/s.

   ```
   huawei(config)#dba-profile add profile-name ftth_dba type3 assure 8192 max 20480
   ```

2. Configure an ONT line profile.

   Create a GPON ONT line profile, named **ftth**, and bind it to the DBA profile **ftth_dba**.

   ```
   huawei(config)#ont-lineprofile gpon profile-name ftth
   huawei(config-gpon-lineprofile-1)#tcont 4 dba-profile-name ftth_dba
   ```


Copyright © Huawei Technologies Co., Ltd.

```
huawei(config-gpon-lineprofile-1)#gem add 11 eth tcont 4
huawei(config-gpon-lineprofile-1)#gem add 12 eth tcont 4
huawei(config-gpon-lineprofile-1)#gem add 13 eth tcont 4
huawei(config-gpon-lineprofile-1)#gem add 14 eth tcont 4
huawei(config-gpon-lineprofile-1)#commit
huawei(config-gpon-lineprofile-1)#quit
```

3. Configure an ONT service profile.

   Create a GPON ONT service profile, named **ftth**. Configure the capability set of the ETH port and POTS port to **adaptive**. Then the system automatically adapts to the ONT according to the actual capability of the online ONT.

   ```
   huawei(config)#ont-srvprofile gpon profile-name ftth
   huawei(config-gpon-srvprofile-1)#ont-port eth adaptive pots adaptive
   huawei(config-gpon-srvprofile-1)#commit
   huawei(config-gpon-srvprofile-1)#quit
   ```

4. (Optional) Add an alarm profile. In this example, the default alarm profile is used, and therefore the configuration of the alarm profile is not required.

Step 3 Add ONTs.

Connect two ONTs to GPON port 0/1/0. Set the ONT IDs to **1** and **2**, SNs to **32303131D659FD40** and **6877687714852901**, passwords to **0100000001** and **0100000002**, discovery mode for password authentication to **once-on**, and management mode to **OMCI**. Bind the two ONTs to ONT line profile **ftth** and ONT service profile **ftth**.

There are two methods of adding an ONT: add an ONT offline and confirm an automatically discovered ONT.

- Add ONTs offline.

  If the password of an ONT is known, run the **ont add** command to add an ONT offline.

  ```
  huawei(config)#interface gpon 0/1
  huawei(config-if-gpon-0/1)#ont add 0 1 password-auth 0100000001 once-on no-aging
  omci ont-lineprofile-name
   ftth ont-srvprofile-name ftth
  huawei(config-if-gpon-0/1)#ont add 0 2 password-auth 0100000002 once-on no-aging
  omci ont-lineprofile-name
   ftth ont-srvprofile-name ftth
  ```

- Confirm automatically discovered ONTs

  If the password or SN of an ONT is unknown, run the **port** ***portid*** **ont-auto-find** command in GPON mode to enable the ONT auto-discovery function of the GPON port. Then, run the **ont confirm** command to confirm the ONT.

  ```
  huawei(config)#interface gpon 0/1
  huawei(config-if-gpon-0/1)#port 0 ont-auto-find enable
  huawei(config-if-gpon-0/1)#display ont autofind 0
    //After this command is executed, the information about all ONTs connected to
  the GPON port through optical splitters is displayed.

  huawei(config-if-gpon-0/1)#ont confirm 0 ontid 1 sn-auth 32303131D659FD40 omci
  ont-lineprofile-name
   ftth ont-srvprofile-name ftth
  huawei(config-if-gpon-0/1)#ont confirm 0 ontid 2 sn-auth 6877687714852901 omci
  ont-lineprofile-name
   ftth ont-srvprofile-name ftth
  ```


Copyright © Huawei Technologies Co., Ltd.

NOTE

If multiple ONTs of the same type bound to the same line profile or service profile are connected to the same port, you can bulk add ONTs by bulk confirming automatically discovered ONTs to make configuration easier and more efficient. To do so, the preceding command can be modified as follows:

```
huawei(config-if-gpon-0/1)#ont confirm 0 all sn-auth omci ont-lineprofile-name
ftth
ont-srvprofile-name ftth
```

- (Optional) Bind the alarm profile to the ONT.

  The default profile 1 is used in this example.

```
huawei(config-if-gpon-0/1)#ont alarm-profile 0 1 profile-id 1
huawei(config-if-gpon-0/1)#ont alarm-profile 0 2 profile-id 1
```

Step 4 Check ONT status.

After an ONT is added, run the **display ont info** command to query the current status of the ONT. Ensure that **Config flag** of the ONT is **active**, **Run State** is **online**, **Config state** is **normal**, and **Match state** is **match**.

```
huawei(config-if-gpon-0/1)#display ont info 0 1
  ------------------------------------------------------------------------
  F/S/P                : 0/1/0
  ONT-ID               : 1
  Control flag         : active    //Indicates that the ONT is
activated.
  Run state            : online    //Indicates that the ONT goes online
successfully.
  Config state         : normal    //Indicates that the configuration state of the
ONT is normal.
  Match state          : match     //Indicates that the capability profile bound to
the ONT is consistent with the actual capability of the ONT.
...//The rest of the response information is omitted.
```

When **Config state** is **failed**, **Run state** is **offline**, or **Match state** is **mismatch**:

- If **Control flag** is **deactive**, run the **ont active** command in GPON mode to activate the ONU.
- If **Run state** is **offline**, a physical line may be broken or the optical module may be damaged. Check the line and the optical module.
- If **Config state** is **failed**, the configured ONU capability exceeds the actual ONU capability. In this case, run the **display ont failed-configuration** command in the diagnose mode to check the failed configuration item and the failure cause. Then, rectify the fault accordingly.
- If the ONU does not match, that is, **Match state** is **mismatch**, the port types and number of ports undermatch the actual port types and number of ports supported by the ONU. In this case, run the **display ont capability** command to query the actual capability of the ONU, and then select one of the following modes to modify the ONU configuration:
  - Create a proper ONU profile according to the actual capability of the ONU, and then run the **ont modify** command to modify the configuration data of the ONU.
  - Modify the ONU profile according to the actual capability of the ONU and save the modification. Then, the ONU automatically recovers the configuration successfully.

Step 5 Configure the traffic profile for the HSI service.

```
huawei(config)#traffic table ip name ftth_hsi cir 4096 priority 0 priority-policy
local-setting
```

Step 6 Configure the service port for the HSI service.

Copyright © Huawei Technologies Co., Ltd.

Table 19-10 Scenario plan

Scenario	VLAN Plan	VLAN Translation Policy
Scenario 1	Double-tagged VLAN ● S-VLAN ID: 100 ● S-VLAN type: smart ● S-VLAN attribute: stacking ● CVLAN ID: 1001 ● C'-VLAN ID: 1010-1011	ONT: ONTs configure the VLAN and add the same C-VLAN tag to packets. All ONTs are in the same C-VLAN. OLT: The OLT performs VLAN translation: C<->S+C'. The C'-VLAN of every ONT differs from each other.
Scenario 2	Double-tagged VLAN ● S-VLAN: 100 ● S-VLAN type: smart ● S-VLAN attribute: stacking ● C-VLAN ID: 1001-1002	ONT: ONTs transparently transmit untagged packets on the user side. OLT: The OLT adds two VLAN tags (S+C) to packets. The C-VLAN of every ONT differs from each other.

- Scenario 1:

  Configure the mapping between a GEM port and a VLAN. The service flow of C-VLAN 1001 is mapped to GEM port 14 in the ONT line profile.

  ```
  huawei(config)#ont-lineprofile gpon profile-name ftth
  huawei(config-gpon-lineprofile-1)#gem mapping 14 0 vlan 1001
  huawei(config-gpon-lineprofile-1)#commit
  huawei(config-gpon-lineprofile-1)#quit
  ```

  Configure the VLAN of the Ethernet port on the ONT. If the ONT is connected to the PC through Ethernet port 1, add Ethernet port 1 to VLAN 1001 in the ONT service profile.

  ```
  huawei(config)#ont-srvprofile gpon profile-name ftth
  huawei(config-gpon-srvprofile-1)#port vlan eth 1 1001
  huawei(config-gpon-srvprofile-1)#commit
  huawei(config-gpon-srvprofile-1)#quit
  ```

  Configure the native VLAN of the ONT port. Set the native VLAN ID of Ethernet port 1 to 1001.

  ```
  huawei(config)#interface gpon 0/1
  huawei(config-if-gpon-0/1)#ont port native-vlan 0 1 eth 1 vlan 1001
  huawei(config-if-gpon-0/1)#ont port native-vlan 0 2 eth 1 vlan 1001
  huawei(config-if-gpon-0/1)#quit
  ```

  Create an Internet access service VLAN and add an upstream port to it. Add upstream port 0/19/0 to VLAN 100.

  ```
  huawei(config)#vlan 100 smart
  huawei(config)#vlan attrib 100 stacking
  huawei(config)#port vlan 100 0/19 0
  ```

  Create service flows. Set the service VLAN to 100, GEM port ID to 14, and user VLAN to 1001. Use traffic profile ftth_hsi.

Copyright © Huawei Technologies Co., Ltd.

```
huawei(config)#service-port vlan 100 gpon 0/1/0 ont 1 gemport 14 multi-service
user-vlan 1001 tag-transform translate-and-add inner-vlan 1010 inbound traffic-
table name
ftth_hsi outbound traffic-table name ftth_hsi
huawei(config)#service-port vlan 100 gpon 0/1/0 ont 2 gemport 14 multi-service
user-vlan 1001 tag-transform translate-and-add inner-vlan 1011 inbound traffic-
table name
ftth_hsi outbound traffic-table name ftth_hsi
```

- Scenario 2:

  Configure the mapping between a GEM port and an Ethernet port on the ONT. Map the service flow of Ethernet port 1 to GEM port 14 in the ONT line profile.

  ```
  huawei(config)#ont-lineprofile gpon profile-name ftth
  huawei(config-gpon-lineprofile-1)#mapping mode port
  huawei(config-gpon-lineprofile-1)#gem mapping 14 0 eth 1
  huawei(config-gpon-lineprofile-1)#commit
  huawei(config-gpon-lineprofile-1)#quit
  ```

  Configure the ONT packet processing mode. If the ONT is connected to the PC through Ethernet port 1, In the ONT service profile, set the packet transmission mode to TAG transparent transmission for Ethernet port 1.

  ```
  huawei(config)#ont-srvprofile gpon profile-name ftth
  huawei(config-gpon-srvprofile-1)#port vlan eth 1 transparent
  huawei(config-gpon-srvprofile-1)#commit
  huawei(config-gpon-srvprofile-1)#quit
  ```

  Create an Internet access service VLAN and add an upstream port to it. Add upstream port 0/19/0 to VLAN 100.

  ```
  huawei(config)#vlan 100 smart
  huawei(config)#vlan attrib 100 stacking
  huawei(config)#port vlan 100 0/19 0
  ```

  Create service flows. Set S-VLAN ID to 100 and GEM port ID to 14. Use traffic profile ftth_hsi.

  ```
  huawei(config)#service-port vlan 100 gpon 0/1/0 ont 1 gemport 14 multi-service
  user-vlan untagged tag-transform add-double inner-vlan 1001 inbound traffic-
  table
   name ftth_hsi outbound traffic-table name ftth_hsi
  huawei(config)#service-port vlan 100 gpon 0/1/0 ont 2 gemport 14 multi-service
  user-vlan untagged tag-transform add-double inner-vlan 1002 inbound traffic-
  table
   name ftth_hsi outbound traffic-table name ftth_hsi
  ```

Step 7 Configure the traffic profile for the voice service.

```
huawei(config)#traffic table ip name ftth_voip cir off priority 5 priority-policy
 local-setting
```

Step 8 Configure the VLAN translation policy and service flows for the voice service.

1. Perform this step in the **bridging ONT (single VLAN tag)** scenario.

Table 19-11 Data plan

Scenario	VLAN Plan	VLAN Translation Policy
Bridging ONT	Single VLAN tag ● VLAN ID: 300 ● VLAN type: smart ● VLAN attribute: common	ONT: provides the VoIP service and uses the same SVLAN.

Copyright © Huawei Technologies Co., Ltd.

Configure the mapping relationship between a GEM port and a VLAN. The service flow of user VLAN 300 is mapped to GEM port 12 in the ONT line profile.

```
huawei(config)#ont-lineprofile gpon profile-name ftth
huawei(config-gpon-lineprofile-1)#gem mapping 12 2 vlan 300
huawei(config-gpon-lineprofile-1)#commit
huawei(config-gpon-lineprofile-1)#quit
```

Create a service VLAN and add an upstream port to it. Add upstream port 0/19/0 to VLAN 300.

```
huawei(config)#vlan 300 smart
huawei(config)#port vlan 300 0/19 0
```

Create service flows. Set the service VLAN to 300, GEM port ID to 12, and user VLAN to 300, and use traffic profile **ftth_voip**.

```
huawei(config)#service-port vlan 300 gpon 0/1/0 ont 1 gemport 12 multi-service
 user-vlan 300 inbound traffic-table name ftth_voip outbound traffic-table
name
ftth_voip
huawei(config)#service-port vlan 300 gpon 0/1/0 ont 2 gemport 12 multi-service
 user-vlan 300 inbound traffic-table name ftth_voip outbound traffic-table
name
ftth_voip
```

2. Perform this step in the **bridging ONT (double VLAN tags)** scenario.

Table 19-12 Data plan

Scenario	VLAN Plan	VLAN Translation Policy
Bridging ONT	Double VLAN tags ● SVLAN ID: 300 ● SVLAN type: smart ● SVLAN attribute: stacking ● CVLAN ID: 3001	ONT: provides the VoIP service and uses the same CVLAN. A CVLAN identifies a VoIP service. OLT: implements VLAN translation: C<->S+C.

Configure the mapping relationship between a GEM port and a VLAN. The service flow of user VLAN 3001 is mapped to GEM port 12 in the ONT line profile.

```
huawei(config)#ont-lineprofile gpon profile-name ftth
huawei(config-gpon-lineprofile-1)#gem mapping 12 2 vlan 3001
huawei(config-gpon-lineprofile-1)#commit
huawei(config-gpon-lineprofile-1)#quit
```

Create a service VLAN and add an upstream port to it. Add upstream port 0/19/0 to VLAN 300.

```
huawei(config)#vlan 300 smart
huawei(config)#vlan attrib 300 stacking
huawei(config)#port vlan 300 0/19 0
```

Create service flows. Set the service VLAN to 300, GEM port ID to 12, and user VLAN to 3001, and use traffic profile **ftth_voip**.

```
huawei(config)#service-port vlan 300 gpon 0/1/0 ont 1 gemport 12 multi-
service
user-vlan 3001 tag-transform default inbound traffic-table name ftth_voip
```


Copyright © Huawei Technologies Co., Ltd.

```
outboun
d traffic-table name ftth_voip
huawei(config)#service-port vlan 300 gpon 0/1/0 ont 2 gemport 12 multi-
service
user-vlan 3001 tag-transform default inbound traffic-table name ftth_voip
outboun
d traffic-table name ftth_voip
```

Step 9 Configure ONT voice service profiles.

ONT voice service profiles include the interface common profile, MGC interface profile, and POTS port profile.

- Interface common profile: saves common attributes of an ONT voice interface, including the fax mode, fax/modem negotiation mode, and priority of the coding and decoding mode.
- MGC interface profile: saves the IP address or domain name of the MGC, protocol port ID of the MGC transport layer to which the MG interface belongs, and DSCP priority of media packets.
- POTS port profile: saves physical attributes of a POTS port on an ONT, including the impedance, transmitting gain, receiving gain, and signaling type of the POTS port.

1. Configure an interface common profile.

   Run the **display ont-mg-attribute-profile** command to query the existing interface common profile in the system. If the existing interface common profile in the system does not meet the requirements, run the **ont-mg-attribute-profile add** command to add an interface common profile.

   In this example, the default interface common profile, namely interface common profile 1 is used.

2. Configure an MGC interface profile.

   Run the **display ont-mgc-profile** command to query the existing MGC interface profile in the system. If the existing MGC interface profile in the system does not meet the requirements, run the **ont-mgc-profile add** command to add an MGC interface profile.

   Create MGC interface profile 2, set the IP address of the MGC to 200.200.200.200, and use default values for other parameters.

   ```
   huawei(config)#ont-mgc-profile add profile-id 2 primary-mgc 200.200.200.200
   ```

3. Configure a POTS port profile.

   Run the **display ont-pots-profile** command to query the existing POTS port profile in the system. If the existing POTS port profile in the system does not meet the requirements, run the **ont-pots-profile add** command to add a POTS port profile.

   In this example, the default POTS port profile, namely POTS port profile 1 is used.

Step 10 Configure the IP addresses of ONT H.248 users.

For ONT 1 and ONT 2, configure the IP address obtaining mode to the dhcp mode, set the management VLAN to VLAN 20, and use default values for other parameters.

```
huawei(config)#interface gpon 0/1
huawei(config-if-gpon-0/1)#ont ipconfig 0 1 dhcp vlan 20
huawei(config-if-gpon-0/1)#ont ipconfig 0 2 dhcp vlan 20
```

Step 11 Configure H.248 PSTN users.

1. Add an H.248 interface and apply an MGC interface profile to the interface.

   For ONT 1 and ONT 2, set the MG ID to 1, apply MGC interface profile 2 to ONT 1 and ONT 2, and use default values for other parameters.

Copyright © Huawei Technologies Co., Ltd.

If parameters of an MGC interface profile are changed, the MGC interface profile must be reapplied to the ONT so that the changed parameters can take effect.

```
huawei(config-if-gpon-0/1)#if-h248 add 0 1 1 mgc-profile profile-id 2
huawei(config-if-gpon-0/1)#if-h248 add 0 2 1 mgc-profile profile-id 2
```

2. Add PSTN users.

   For ONT 1 and ONT 2, create a PSTN user, set the MG ID to 1 (identical to the MG ID of the H.248 interface), and set the physical terminal port ID to A0 and A1.

```
huawei(config-if-gpon-0/1)#mgpstnuser add 0 1 1 mgid 1 terminalid A0
huawei(config-if-gpon-0/1)#mgpstnuser add 0 2 1 mgid 1 terminalid A1
```

   Run the **display mgpstnuser attribute** command to check whether the configuration of the PSTN user is properly set.

```
huawei(config-if-gpon-0/1)#display mgpstnuser attribute 0 1 1

---------------------------------------------------------------------------
  F/S/P                       : 0/1/0
  ONT ID                      : 1
  Port ID                     : 1

  MG ID                       : 1
  Terminal ID                 : A0
...//The rest of the response information is omitted.

huawei(config-if-gpon-0/1)#display mgpstnuser attribute 0 2 1

---------------------------------------------------------------------------
  F/S/P                       : 0/1/0
  ONT ID                      : 2
  Port ID                     : 1

  MG ID                       : 1
  Terminal ID                 : A1
...//The rest of the response information is omitted.
```

Step 12 Apply ONT voice service profiles

After ONT voice service profiles are applied, if parameters in those profiles are changed, those profiles must be reapplied so that the changed parameters can take effect.

1. Apply an interface common profile.

   Run the **if-h248 attribute** command to apply an interface common profile to an H.248 interface or configure the interface customized parameters, or run the **ont-if-h248 bat-apply** command to bulk apply the interface common profiles to H.248 interfaces. If you use these two commands to apply the interface common profiles or configure the interface customized parameters repeatedly, the last configurations take effect.

   In this example, the default interface common profile, namely interface common profile 1 is used.

2. Apply a POTS port profile.

   Run the **pstnport electric** command to apply a POTS port profile to an H.248 interface or configure the interface customized parameters, or run the **ont-pstnport electric bat-apply** command to bulk apply the POTS port profiles to H.248 interfaces. If you use these two commands to apply the POTS port profiles or configure the interface customized parameters repeatedly, the last configurations take effect.

   In this example, the default POTS port profile, namely POTS port profile 1 is used.

Step 13 (Optional) Configure the H.248 user codec.

Copyright © Huawei Technologies Co., Ltd.

Run the **mgpstnuser codec** command to configure the H.248 user codec. The H.248 user codec will not be configured independently in this example.

Step 14 Configure the traffic profile for the IPTV service.

```
huawei(config)#traffic table ip index 8 cir off priority 4 priority-policy
local-setting
```

Step 15 Configure the VLAN translation policy and service port for the multicast service.

Configure the mapping relationship between a GEM port and an Ethernet port on the ONT. If the ONT is connected to the STB through Ethernet port 2, map the service flow of Ethernet port 2 to GEM port 13 in the ONT line profile.

```
huawei(config)#ont-lineprofile gpon profile-name ftth
huawei(config-gpon-lineprofile-1)#mapping mode port
huawei(config-gpon-lineprofile-1)#gem mapping 13 1 eth 2
huawei(config-gpon-lineprofile-1)#commit
huawei(config-gpon-lineprofile-1)#quit
```

Configure the VLAN of the Ethernet port on the ONT. If the ONT is connected to the STB through Ethernet port 2, add Ethernet port 2 to VLAN 1000.

```
huawei(config)#ont-srvprofile gpon profile-name ftth
huawei(config-gpon-srvprofile-1)#port vlan eth 2 1000
huawei(config-gpon-srvprofile-1)#multicast-forward untag
huawei(config-gpon-srvprofile-1)#commit
huawei(config-gpon-srvprofile-1)#quit
```

Configure the native VLAN of the ONT port. If the ONT is connected to the STB through Ethernet port 2, the native VLAN ID is 1000.

```
huawei(config)#interface gpon 0/1
huawei(config-if-gpon-0/1)#ont port native-vlan 0 1 eth 2 vlan 1000
huawei(config-if-gpon-0/1)#ont port native-vlan 0 2 eth 2 vlan 1000
huawei(config-if-gpon-0/1)#quit
```

Create a service VLAN and add an upstream port to it. Add upstream port 0/19/0 to VLAN 1000.

```
huawei(config)#vlan 1000 smart
huawei(config)#port vlan 1000 0/19 0
```

Create service flows. Set the service VLAN to 1000, GEM port ID to 13, and user VLAN to untagged, and use traffic profile 8.

```
huawei(config)#service-port 1 vlan 1000 gpon 0/1/0 ont 1 gemport 13 multi-service
 user-vlan untagged rx-cttr 8 tx-cttr 8
huawei(config)#service-port 2 vlan 1000 gpon 0/1/0 ont 2 gemport 13 multi-service
 user-vlan untagged rx-cttr 8 tx-cttr 8
```

Step 16 Create an MVLAN and configure the IGMP version.

Set the IGMP version for the MVLAN to IGMP IPv6 v2.

```
huawei(config)#multicast-vlan 1000
huawei(config-mvlan1000)#igmp ipv6 version v2
  This operation will delete all IPv6 programs with source IP addresses in the
current multicast VLAN
  Are you sure to change current IGMP IPv6 version? (y/n)[n]:y
  Command is being executed. Please wait...
  Command has been executed successfully
```

Step 17 Configure a program library.

Set the mode for obtaining multicast programs to dynamic.

Copyright © Huawei Technologies Co., Ltd.

NOTE

You can set the mode for obtaining multicast programs to dynamic only when the IGMP mode is off.

```
huawei(config-mvlan1000)#igmp ipv6 mode off
  Are you sure to close IGMP IPv6? (y/n)[n]:y
  Command is being executed. Please wait...
  Command has been executed successfully

huawei(config-mvlan1000)#igmp ipv6 match mode disable
  Command has been executed successfully
```

(Optional) Set the address range for the dynamic programs. If you need to limit the address range of dynamic programs, perform this operation. For example, set the address range of dynamic programs to ff15::-ff15::ffff.

```
huawei(config-mvlan1000)#igmp ipv6 match group ipv6 ff15:: to-ipv6 ff15::ffff
```

Step 18 Set the IGMP IPv6 mode.

Select the IGMP IPv6 proxy mode.

```
huawei(config-mvlan1000)#igmp ipv6 mode proxy
  Are you sure to change IGMP IPv6 mode? (y/n)[n]:y
  Command is being executed. Please wait...
  Command has been executed successfully
```

Step 19 Configure the IGMP upstream port.

Set the IGMP upstream port ID to 0/19/0 and working mode to **default**. Protocol packets are transmitted to all the IGMP upstream ports in the multicast VLAN.

```
huawei(config-mvlan1000)#igmp uplink-port 0/19/0
huawei(config-mvlan1000)#btv
huawei(config-btv)#igmp uplink-port-mode default
Are you sure to change the uplink port mode?(y/n)[n]:y
```

Step 20 Configure multicast users.

Add service ports 1 and 2 as multicast users.

```
huawei(config-btv)#igmp policy service-port 1 normal
huawei(config-btv)#igmp policy service-port 2 normal
huawei(config-btv)#igmp user add service-port 1
huawei(config-btv)#igmp user add service-port 2
huawei(config-btv)#multicast-vlan 1000
huawei(config-mvlan1000)#igmp multicast-vlan member service-port 1
huawei(config-mvlan1000)#igmp multicast-vlan member service-port 2
huawei(config-mvlan1000)#quit
```

Step 21 Configure the traffic profile for the VoD service.

```
huawei(config)#traffic table ip index 8 cir off priority 4 priority-policy
local-setting
```

Step 22 Configure the VLAN translation policy and service port for the VoD service.

Configure the mapping relationship between a GEM port and a VLAN. The service flow of user VLAN 1100 is mapped to GEM port 13 in the ONT line profile.

```
huawei(config)#ont-lineprofile gpon profile-name ftth
huawei(config-gpon-lineprofile-1)#gem mapping 13 4 vlan 1100
huawei(config-gpon-lineprofile-1)#commit
huawei(config-gpon-lineprofile-1)#quit
```

Configure the VLAN of the Ethernet port on the ONT. If the ONT is connected to the STB through Ethernet port 2, add Ethernet port 2 to VLAN 1100.

```
huawei(config)#ont-srvprofile gpon profile-name ftth
huawei(config-gpon-srvprofile-1)#port vlan eth 2 1100
```


Copyright © Huawei Technologies Co., Ltd.

```
huawei(config-gpon-srvprofile-1)#commit
huawei(config-gpon-srvprofile-1)#quit
```

Configure the native VLAN of the ONT port. If the ONT is connected to the STB through Ethernet port 2, the native VLAN ID is 1100.

```
huawei(config-if-gpon-0/1)#ont port native-vlan 0 1 eth 2 vlan 1100
huawei(config-if-gpon-0/1)#ont port native-vlan 0 2 eth 2 vlan 1100
huawei(config-if-gpon-0/1)#quit
```

Create a service VLAN and add an upstream port to it. Add upstream port 0/19/0 to VLAN 1100.

```
huawei(config)#vlan 1100 smart
huawei(config)#port vlan 1100 0/19 0
```

Create service flows. Set the service VLAN to 1100, GEM port ID to 13, and VLAN translation mode to transparent transmission, and use traffic profile 8.

```
huawei(config)#service-port 3 vlan 1100 gpon 0/1/0 ont 1 gemport 13 rx-cttr 8 tx-
cttr 8 tag-transform transparent
huawei(config)#service-port 4 vlan 1100 gpon 0/1/0 ont 2 gemport 13 rx-cttr 8 tx-
cttr 8 tag-transform transparent
```

Step 23 (Optional) Configure the PITP function for PPPoE.

```
huawei(config)#raio-mode common pitp-pmode
huawei(config)#pitp enable pmode
```

Step 24 (Optional) Configure the DHCP option function for IPoE.

```
huawei(config)#raio-mode common dhcp-option82      //For DHCPv4 packets
huawei(config)#dhcp option82 enable                      //For DHCPv4 packets
huawei(config)#raio-mode common dhcpv6-option            //For DHCPv6 packets
huawei(config)#dhcpv6 option enable                      //For DHCPv6 packets
```

Step 25 Save the configuration on the OLT side.

```
huawei(config)#save
```

----End

19.6 Configuring IPv6 Services in the FTTH (Gateway ONT) Scenario

This section describes the methods for configuring IPv6 services in the FTTH (gateway ONT) scenario.

19.6.1 Application Scenarios

The FTTH (gateway ONT) supports multiple IPv6 HSI and IPTV service solutions.

FTTH (Gateway ONT) Application Scenarios

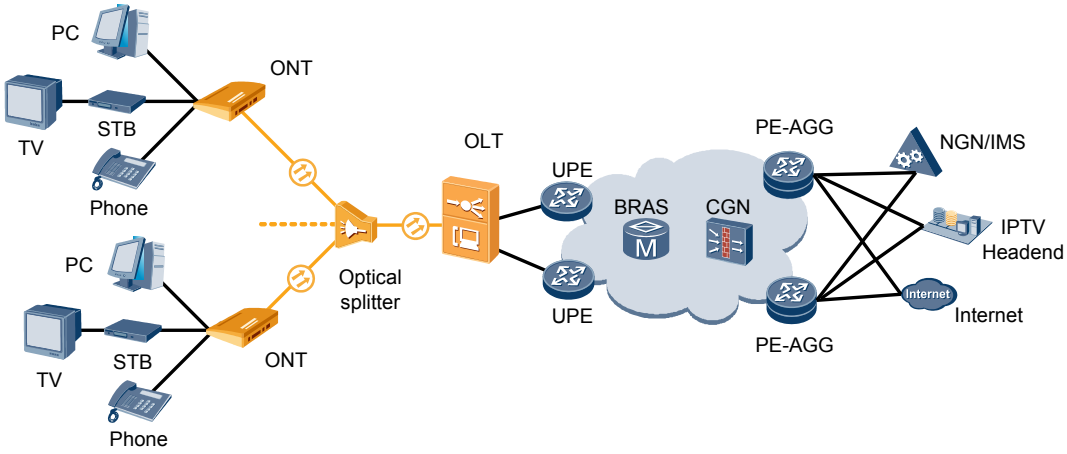
As shown in **Figure 19-7**, the FTTH (gateway ONT) works with upper-layer devices to support DS+NAT+PPPoE, DS+NAT+IPoE/DS-Lite+NAT+PPPoE HSI and DS+IPoE/DS+PPPoE IPTV services in the Huawei fixed network IPv6 solution.

- Voice service: The ONT with a bulit-in voice module can provide VoIP services for users. The ONT can process VoIP services using IPv4.

Copyright © Huawei Technologies Co., Ltd.

- Internet service: The PC and BRAS support the IPv4/IPv6 dual-stack and are connected using the PPPoE or IPoE dial-up. The OLT and ONT have the same forwarding and configuration methods for both IPv4 and IPv6 user services. The only difference is that commands for configuring the ACL and security (DHCP option and anti-IP spoofing) features are different.
  - For DS+NAT+PPPoE and DS+NAT+IPoE solutions, both the ONT and BRAS support IPv4/IPv6 dual-stack and are connected using PPPoE or IPoE. The ONT must enable the IPv4 and IPv6 simultaneously at the WAN port. The OLT performs Layer 2 forwarding for both IPv4 and IPv6 user services, which are configured almost in the same way. The only difference is that commands for configuring the ACL and security features (DHCP option and anti-IP spoofing) are different.
  - For DS-Lite+PPPoE, the BRAS must support IPv4/IPv6 dual-stack while the ONT supports the DS-Lite. The ONT and BRAS are connected using PPPoE. The HGW encapsulates IPv4 service packets into the 4in6 tunnel, and transmits them to the CGN for decapsulation. The ONT must enable DS-Lite at the WAN port. The OLT performs Layer 2 forwarding for both IPv4 and IPv6 user services, which are configured almost in the same way. The only difference is that commands for configuring DHCP option and anti-IP spoofing are different.
- IPTV service: The STB supports IPv4/IPv6 dual-stack and carries IPTV services using either IPv4 or IPv6.
  - When the STB uses IPoE and the OLT functions as the multicast duplicate point, the process for configuring IPv6 and IPv4 multicast services is the same, but commands are different. The OLT and ONU perform bridge forwarding for both IPv4 and IPv6 user services, which can be configured almost in the same way.
  - When the STB uses PPPoE, it directly connects to the BRAS by PPPoE. The OLT and ONT only forward PPPoE services instead of processing multicast services. This solution is not recommended.

Figure 19-7 FTTH (gateway ONT) service networking



19.6.2 Data Plan

This section describes the security, device management data, QoS, Internet service data, voice service data, and IPTV service data planning.

Copyright © Huawei Technologies Co., Ltd.

Security Planning

Security planning includes system security, user security, and service security, ensuring user services are provided properly from different dimensions.

In the FTTH (gateway ONT) networking scenario, only anti-IP spoofing and DHCP option of IPv6 and IPv4 services are different.

Anti-IP spoofing: This function needs to be configured separately for IPv6 services.

The anti-IP spoofing function can be enabled or disabled at three levels. This function takes effect only when it is enabled at all the three levels.

1. Global level: Run the **security anti-ipv6spoofing enable** command in global config mode.
2. VLAN level: Run the **security anti-ipv6spoofing enable** command in VLAN service profile mode.
3. Service port level: Run the **security anti-ipv6spoofing service-port** *serviceport-id* **enable** command.

DHCP option: The DHCP option for IPv4 is DHCPv4 option 82 and for IPv6 is DHCPv6 option 18/37.

The DHCPv6 option18 and option37 functions can be enabled or disabled at two levels. This function takes effect only when it is enabled at both levels.

1. Global level: Run the **dhcpv6 option enable** command in global config mode.
2. VLAN level: Run the **dhcpv6 option enable** command in VLAN service profile mode.

Device Management Data Planning

Device management data planning includes the management channel and IP address planning. The management channel for IPv6 and IPv4 services are the same.

Planning	Device or Service	Solution Introduction
Management channel	OLT	The device management uses single-tagged VLANs on the entire network.

Copyright © Huawei Technologies Co., Ltd.

Planning	Device or Service	Solution Introduction
IP address planning (gateway ONT)	Internet	● IPv4 address: An ONT obtains the IPv4 address from the BRAS using PPPoE or DHCP. If IPoE dial-up is used, the static address can be configured. Meanwhile, as the DHCP server, the ONT allocates private network IP addresses to PCs. The NAT function enables these PCs to go online by sharing the IPv4 address allocated by the BRAS. – The BRAS can allocate a public network IP address to an ONT. – The BRAS can allocate a private network address to an ONT. The private network address is translated to the public network address by CGN (NAT44). ● IPv6 address: An ONT obtains the IPv6 address from the BRAS using PPPoE, SLAAC, or DHCPv6. If IPoE dial-up is used, the static address can be configured. Meanwhile, the ONT as the DHCP server obtains the prefix of an IPv6 address, and allocates IPv6 addresses to connected PCs using the network cable or WiFi.
	IPTV service	● If the IPv4 protocol is used, an STB obtains the IP address from the BRAS using DHCP. ● If the IPv6 protocol is used, the STB obtains the IP address in either of the following ways: – Obtains the IP address from the BRAS using DHCPv6. – Obtains the IP address from the BRAS using SLAAC.
	VoIP service	The IPv4 protocol is still used. The ONT functions as the DHCP client to obtain an IP address from the DHCP server, or the NMS issues a static IP address to the ONT using the configuration file. Voice media/signaling flows at multiple POTS ports share one IP address. Media flows are classified by port.
	TR069 management	The IPv4 protocol is still used. For scenarios in which TR069 is required for management maintenance and service provisioning, the ONT functions as the DHCP client to obtain a public network IP address from the DHCP server to connect the TR069 server ACS.

Copyright © Huawei Technologies Co., Ltd.

QoS Planning

The E2E QoS planning includes the flow classification, marking/scheduling policy, traffic monitoring, and DBA policy.

When the IPv6 protocol is used, the QoS planning is the same for both IPv6 and IPv4.

- Management service: IPv4
- Voice service: IPv4
- IPTV service: One user uses either IPv6 or IPv4 at one time. The QoS planning for IPv6 and IPv4 IPTV services is the same.
- Internet service: It is recommended that access devices use one flow to carry IPv6 and IPv4 Internet services. The QoS planning is the same for the flow that carries both IPv6 and IPv4 Internet services and the flow that carries only the IPv4 Internet service.

Internet Service Planning

The Internet service planning includes the VLAN and VLAN switching policy planning in different networking scenarios.

IPv6 and IPv4 Internet services: It is recommended that devices use one flow to carry IPv6 and IPv4 Internet services. This facilitates the control of the aggregate rate for IPv6 and IPv4 Internet services. The QoS planning is the same for the flow that carries both IPv6 and IPv4 Internet services and the flow that carries only the IPv4 Internet service.

Voice Service Data Planning

Voice service data planning includes the VLAN/VLAN switching policy planning in different networking scenarios, and voice protocol planning.

Even after IPv6 is used, the device still uses IPv4 to implement voice services.

IPTV Service Data Planning

IPTV service data planning includes the VLAN/VLAN switching policy planning in different networking scenarios, and IPTV service planning.

When the IPv6 protocol is used, one IPTV user uses either IPv6 or IPv4 at one time. The VLAN data planning for IPv6 is consistent with that for IPv4. IGMP protocol differences are demonstrated in the configuration procedure.

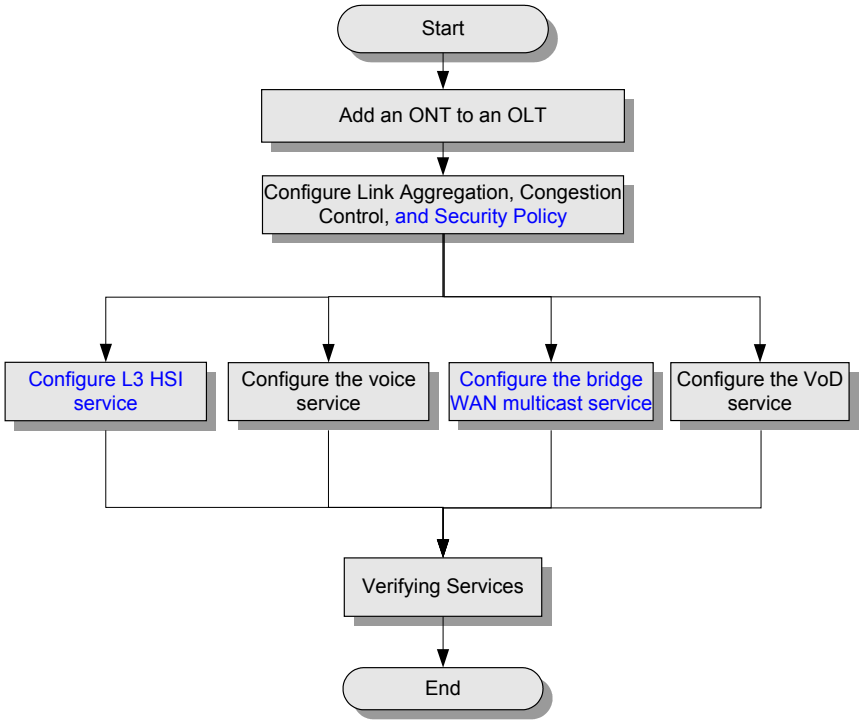
19.6.3 Configuration Procedure

This section describes IPv6 configuration procedure, and compares it with the IPv4 configuration procedure.

FTTH (Gateway ONT) Configuration Procedure

After IPv6 is introduced to the FTTH (gateway ONT) scenario, the service configuration procedure is shown in the following figure. When IPv6 is introduced, the configurations for security features, Layer 3 Internet services, bridging WAN multicast services are different from those of IPv4. For differences, see **19.2 Configuration Difference Between IPv6 and IPv4**.

Copyright © Huawei Technologies Co., Ltd.



NOTE

Texts in blue show the configuration difference between IPv6 and IPv4.

19.6.4 Configuration Example

Introduce the end-to-end service configuration based on the FTTH (Gateway ONT) networking and the corresponding data plan.

Key Messages for Configuration

In this example, two ONTs are connected to the same PON port of the OLT. Triple play services are required

- Even after IPv6 is used, the voice service is still realized by IPv4.
- Even after IPv6 is used, the OLT implement Layer 2 forwarding for HSI service in this networking, irrespective of whether the access service is IPv4 or IPv6. Service configurations for IPv4 and IPv6 are the same. For the HSI service from one end user, one service flow is used to carry IPv6 and IPv4 Internet services, and the same service VLAN is used. The gateway ONT requires specific configuration to enable the IPv4/IPv6 dual stack or the DS-Lite for the HSI service.
- For multicast service, the OLT is the node to make multicast duplication. The configuration procedure is the same for IPv4 multicast and IPv6 multicase. The IPv4 multicast service and IPv6 multicast service can be configured in the same multicast VLAN on the OLT equipment.

Data plan on the OLT side

Web or the NMS is recommended to configure the gateway ONT layer 3 HSI service. CLI through the OLT is recommended to configure the gateway ONT voice service. The WAN interface for multicast service on the ONT is configured by iTMS.

Copyright © Huawei Technologies Co., Ltd.

Item	Data	Memo
ONT data plan		
DBA profile	Profile name: ftth_dba Profile type: type3 Assured bandwidth: 8 Mbit/s Maximum bandwidth: 20 Mbit/s	The ONTs are connected to the OLT through the GPON port.
ONT line profile	Profile name: ftth T-CONT ID: 4 GEM port ID for management services: 11 GEM port ID for voice services: 12 GEM port ID for video services: 13 GEM port ID for Internet access services: 14	
ONT service profile	Profile name: ftth ONT port capability set: adaptive	
Network topology data	PON port: 0/1/0 ONT IDs: 1 and 2	
LAG data plan		
LAG	Ports: 0/19/0 and 0/19/1 Working mode: LACP static aggregation	Configure upstream ports 0/19/0 and 0/19/1 into an aggregation group. Each member port in the aggregation group allocates packets based on the source MAC address.
Queue scheduling data plan		
Queue scheduling	Queue scheduling: strict priority (SQ) mode Priority mapping: mapped into different queues based on priorities	System default is adopted in this example.
Security data plan		
System security	Anti-DOS attack: disabled Anti-ICMP attack: disabled Anti-IP attack: disabled	System default is adopted in this example.

Copyright © Huawei Technologies Co., Ltd.

Item	Data	Memo
User security	Anti-MAC duplicate: disabled Anti-IP sproofing: disabled	System default is adopted in this example.
PPPoE Service security	RAIO Type: PITP P RAIO Mode: common	PITP is recommended for PPPoE.
IPv4oE Service security	RAIO Type: DHCP Option 82 RAIO Mode: common	DHCPv4 option and DHCPv6 option are recommended for IPoE.
IPv6oE Service security	RAIO Type: DHCPv6 Option RAIO Mode: common	
HSI service data plan		
ONT line profile	Profile name: ftth T-CONT ID: 4 GEM port ID: 14	For details, see **19.6.2 Data Plan**.
ONT service profile	Profile name: ftth ONT port capability set: adaptive	
Traffic profile	Profile name: ftth_hsi CIR: 4Mbit/s Priority: 0	
Network topology data	Upstream port: 0/19/0 PON port: 0/1/0 ONT IDs: 1 and 2 ID of the port on the ONT that is connected to the PC: 1	
Voice service data plan		
ONT line profile	Profile name: ftth T-CONT ID: 4 GEM port ID: 12	For details, see **19.6.2 Data Plan**.
ONT service profile	Profile name: ftth ONT port capability set: adaptive	

Copyright © Huawei Technologies Co., Ltd.

Item	Data	Memo
Traffic profile	Profile name: ftth_voip CIR: not limited Priority: 5	
Networking data	IP address of the MGC server: 200.200.200.200/24 Port ID of the MGC server: 2944	
Bridge WAN multicast service data plan		
ONT line profile	Profile name: ftth T-CONT ID: 4 GEM port ID: 13	For details, see **19.6.2 Data Plan**.
ONT service profile	Profile name: ftth ONT port capability set: adaptive	
Traffic profile	ID: 8 802.1p priority: 4 CIR: off (unlimited) Priority-based scheduling policy: local-setting	
VLAN Plan	SVLAN ID: 1000 VLAN type: smart VLAN attribute: common	
VLAN Translation Policy	ONT: duplicates packets based on user ports and multicast VLANs (MVLANs) are stripped off downstream. OLT: duplicates multicast packets based on PON ports with MVLAN unchanged.	
Multicast service data	Multicast protocol: IGMP proxy Multicast version: IGMPv2 Multicast program: dynamic obtaining mode Program address area: ff15::-ff15::ffff	
VOD service data plan		

Copyright © Huawei Technologies Co., Ltd.

Item	Data	Memo
ONT line profile	Profile name: ftth T-CONT ID: 4 GEM port ID: 13	For details, see **19.6.2 Data Plan**.
ONT service profile	Profile name: ftth ONT port capability set: adaptive	
Traffic profile	ID: 8 802.1p priority: 4 CIR: off (unlimited) Priority-based scheduling policy: local-setting	
VLAN Plan	Single VLAN tag ● SVLAN ID: 1100 ● VLAN type: smart ● VLAN attribute: common ● CVLAN: 2001	
VLAN Translation Policy	The ONT adds CVALN tags (configured on the iTMS) to packets: untag<->C. The OLT implements VLAN translation: C<->S.	

Procedure

Step 1 Configure LAG for upstream ports.

Configure upstream ports 0/19/0 and 0/19/1 into an aggregation group. Each member port in the aggregation group allocates packets based on the source MAC address. The working mode is LACP static aggregation.

```
huawei(config)#link-aggregation 0/19 0-1 ingress workmode lacp-static
```

Step 2 Configure GPON ONT profiles.

1. Configure a DBA profile.

   Create the same DBA profile for different types of services. Set the profile name to **ftth_dba**, profile type to **type3**, assured bandwidth to 8 Mbit/s, and maximum bandwidth to 20 Mbit/s.

   ```
   huawei(config)#dba-profile add profile-name ftth_dba type3 assure 8192 max 20480
   ```

2. Configure an ONT line profile.

   Create a GPON ONT line profile, named **ftth**, and bind it to the DBA profile **ftth_dba**.

Copyright © Huawei Technologies Co., Ltd.

```
huawei(config)#ont-lineprofile gpon profile-name ftth
huawei(config-gpon-lineprofile-1)#tcont 4 dba-profile-name ftth_dba
huawei(config-gpon-lineprofile-1)#gem add 11 eth tcont 4
huawei(config-gpon-lineprofile-1)#gem add 12 eth tcont 4
huawei(config-gpon-lineprofile-1)#gem add 13 eth tcont 4
huawei(config-gpon-lineprofile-1)#gem add 14 eth tcont 4
huawei(config-gpon-lineprofile-1)#commit
huawei(config-gpon-lineprofile-1)#quit
```

3. Configure an ONT service profile.

   Create a GPON ONT service profile, named **ftth**. Configure the capability set of the ETH port and POTS port to **adaptive**. Then the system automatically adapts to the ONT according to the actual capability of the online ONT.

   ```
   huawei(config)#ont-srvprofile gpon profile-name ftth
   huawei(config-gpon-srvprofile-1)#ont-port eth adaptive pots adaptive
   huawei(config-gpon-srvprofile-1)#commit
   huawei(config-gpon-srvprofile-1)#quit
   ```

4. (Optional) Add an alarm profile. In this example, the default alarm profile is used, and therefore the configuration of the alarm profile is not required.

Step 3 Add ONTs.

Connect two ONTs to GPON port 0/1/0. Set the ONT IDs to **1** and **2**, SNs to **32303131D659FD40** and **6877687714852901**, passwords to **0100000001** and **0100000002**, discovery mode for password authentication to **once-on**, and management mode to **OMCI**. Bind the two ONTs to ONT line profile **ftth** and ONT service profile **ftth**.

There are two methods of adding an ONT: add an ONT offline and confirm an automatically discovered ONT.

- Add ONTs offline.

  If the password of an ONT is known, run the **ont add** command to add an ONT offline.

  ```
  huawei(config)#interface gpon 0/1
  huawei(config-if-gpon-0/1)#ont add 0 1 password-auth 0100000001 once-on no-aging
  omci ont-lineprofile-name
   ftth ont-srvprofile-name ftth
  huawei(config-if-gpon-0/1)#ont add 0 2 password-auth 0100000002 once-on no-aging
  omci ont-lineprofile-name
   ftth ont-srvprofile-name ftth
  ```

- Confirm automatically discovered ONTs

  If the password or SN of an ONT is unknown, run the **port** ***portid*** **ont-auto-find** command in GPON mode to enable the ONT auto-discovery function of the GPON port. Then, run the **ont confirm** command to confirm the ONT.

  ```
  huawei(config)#interface gpon 0/1
  huawei(config-if-gpon-0/1)#port 0 ont-auto-find enable
  huawei(config-if-gpon-0/1)#display ont autofind 0
    //After this command is executed, the information about all ONTs connected to
  the GPON port through optical splitters is displayed.

  huawei(config-if-gpon-0/1)#ont confirm 0 ontid 1 sn-auth 32303131D659FD40 omci
  ont-lineprofile-name
   ftth ont-srvprofile-name ftth
  huawei(config-if-gpon-0/1)#ont confirm 0 ontid 2 sn-auth 6877687714852901 omci
  ont-lineprofile-name
   ftth ont-srvprofile-name ftth
  ```


Copyright © Huawei Technologies Co., Ltd.

NOTE

If multiple ONTs of the same type bound to the same line profile or service profile are connected to the same port, you can bulk add ONTs by bulk confirming automatically discovered ONTs to make configuration easier and more efficient. To do so, the preceding command can be modified as follows:

```
huawei(config-if-gpon-0/1)#ont confirm 0 all sn-auth omci ont-lineprofile-name
ftth
ont-srvprofile-name ftth
```

- (Optional) Bind the alarm profile to the ONT.

  The default profile 1 is used in this example.

```
huawei(config-if-gpon-0/1)#ont alarm-profile 0 1 profile-id 1
huawei(config-if-gpon-0/1)#ont alarm-profile 0 2 profile-id 1
```

Step 4 Check ONT status.

After an ONT is added, run the **display ont info** command to query the current status of the ONT. Ensure that **Config flag** of the ONT is **active**, **Run State** is **online**, **Config state** is **normal**, and **Match state** is **match**.

```
huawei(config-if-gpon-0/1)#display ont info 0 1
  ------------------------------------------------------------------------
  F/S/P                : 0/1/0
  ONT-ID               : 1
  Control flag         : active    //Indicates that the ONT is
activated.
  Run state            : online    //Indicates that the ONT goes online
successfully.
  Config state         : normal    //Indicates that the configuration state of the
ONT is normal.
  Match state          : match     //Indicates that the capability profile bound to
the ONT is consistent with the actual capability of the ONT.
...//The rest of the response information is omitted.
```

When **Config state** is **failed**, **Run state** is **offline**, or **Match state** is **mismatch**:

- If **Control flag** is **deactive**, run the **ont active** command in GPON mode to activate the ONU.
- If **Run state** is **offline**, a physical line may be broken or the optical module may be damaged. Check the line and the optical module.
- If **Config state** is **failed**, the configured ONU capability exceeds the actual ONU capability. In this case, run the **display ont failed-configuration** command in the diagnose mode to check the failed configuration item and the failure cause. Then, rectify the fault accordingly.
- If the ONU does not match, that is, **Match state** is **mismatch**, the port types and number of ports undermatch the actual port types and number of ports supported by the ONU. In this case, run the **display ont capability** command to query the actual capability of the ONU, and then select one of the following modes to modify the ONU configuration:
  - Create a proper ONU profile according to the actual capability of the ONU, and then run the **ont modify** command to modify the configuration data of the ONU.
  - Modify the ONU profile according to the actual capability of the ONU and save the modification. Then, the ONU automatically recovers the configuration successfully.

Step 5 Configure the traffic profile for the HSI service.

```
huawei(config)#traffic table ip name ftth_hsi cir 4096 priority 0 priority-policy
local-setting
```

Step 6 Configure the VLAN translation policy and the service port for the HSI service.

Copyright © Huawei Technologies Co., Ltd.

Table 19-13 Scenario plan

Scenario	VLAN Plan	VLAN Translation Policy
Scenario 1	Double VLAN tags ● SVLAN ID: 100 ● SVLAN type: smart ● SVLAN attribute: stacking ● CVLAN ID: 1001-1002	ONT: The iTMS factory default setting (untag) is used. OLT: performs VLAN translation: Untag<->S+C. The OLT adds different CVLANs to packets from different ONTs.
Scenario 2	Double VLAN tags ● SVLAN ID: 100 ● SVLAN type: smart ● SVLAN attribute: stacking ● C'VLAN ID: 1010-1011 ● CVLAN ID: 1001	ONT: The iTMS configures CVLANs in a unified manner. OLT: performs VLAN translation: C<->S+C'. The OLT translates CVLANs from different ONTs to different C'VLANs.

- Scenario 1:

  Configure the ONT packet processing mode. In the ONT service profile, set the packet transmission mode to TAG transparent transmission for Ethernet port 1.

```
huawei(config)#ont-srvprofile gpon profile-name ftth
huawei(config-gpon-srvprofile-1)#port vlan eth 1 transparent
huawei(config-gpon-srvprofile-1)#commit
huawei(config-gpon-srvprofile-1)#quit
```

  Create a service VLAN and add an upstream port to it. Add upstream port 0/19/0 to VLAN 100.

```
huawei(config)#vlan 100 smart
huawei(config)#vlan attrib 100 stacking
huawei(config)#port vlan 100 0/19 0
```

  Create service flows. Set SVLAN ID to 100 and GEM port ID to 14. Use traffic profile ftth_hsi.

```
huawei(config)#service-port vlan 100 gpon 0/1/0 ont 1 gemport 14 multi-service
user-vlan untagged tag-transform add-double inner-vlan 1001 inbound traffic-
table name
ftth_hsi outbound traffic-table name ftth_hsi
huawei(config)#service-port vlan 100 gpon 0/1/0 ont 2 gemport 14 multi-service
user-vlan untagged tag-transform add-double inner-vlan 1002 inbound traffic-
table name
ftth_hsi outbound traffic-table name ftth_hsi
```

- Scenario 2:

  Configure the mapping relationship between a GEM port and a VLAN. The service flow of user VLAN 1001 is mapped to GEM port 14 in the ONT line profile.

```
huawei(config)#ont-lineprofile gpon profile-name ftth
huawei(config-gpon-lineprofile-1)#gem mapping 14 0 vlan 1001
huawei(config-gpon-lineprofile-1)#commit
huawei(config-gpon-lineprofile-1)#quit
```


Copyright © Huawei Technologies Co., Ltd.

Create a service VLAN and add an upstream port to it. Add upstream port 0/19/0 to VLAN 100.

```
huawei(config)#vlan 100 smart
huawei(config)#vlan attrib 100 stacking
huawei(config)#port vlan 100 0/19 0
```

Create service flows. Set the service VLAN to 100, GEM port ID to 14, and user VLAN to 1001, and use traffic profile ftth_hsi.

```
huawei(config)#service-port vlan 100 gpon 0/1/0 ont 1 gemport 14 multi-service
user-vlan 1001 tag-transform translate-and-add inner-vlan 1010 inbound traffic-
table name
ftth_hsi outbound traffic-table name ftth_hsi
huawei(config)#service-port vlan 100 gpon 0/1/0 ont 2 gemport 14 multi-service
user-vlan 1001 tag-transform translate-and-add inner-vlan 1011 inbound traffic-
table name
ftth_hsi outbound traffic-table name ftth_hsi
```

Step 7 Configure the traffic profile for the voice service.

```
huawei(config)#traffic table ip name ftth_voip cir off priority 5 priority-policy
 local-setting
```

Step 8 Configure the VLAN translation policy and service port for the voice service.

Table 19-14 Scenario plan

Scenario	VLAN Plan	VLAN Translation Policy
Scenario 1	Single VLAN tag ● SVLAN ID: 300 ● SVLAN type: smart ● SVLAN attribute: common ● CVLAN ID: 300	ONT: The iTMS issues the VLAN of the WAN port or factory default setting is used. OLT: transparently transmits VLAN (CVLAN is the same as the planned SVLAN).
Scenario 2	Single VLAN tag ● SVLAN ID: 300 ● SVLAN type: smart ● SVLAN attribute: common ● CVLAN ID: 3001	ONT: The iTMS issues the VLAN of the WAN port or factory default setting is used. OLT: performs VLAN translation: C<->S (CVLAN is different from the planned SVLAN).

Scenario 1:

Configure the mapping relationship between a GEM port and a VLAN. The service flow of user VLAN 300 is mapped to GEM port 12 in the ONT line profile.

```
huawei(config)#ont-lineprofile gpon profile-name ftth
huawei(config-gpon-lineprofile-1)#gem mapping 12 2 vlan 300
huawei(config-gpon-lineprofile-1)#commit
huawei(config-gpon-lineprofile-1)#quit
```

Create a service VLAN and add an upstream port to it. Add upstream port 0/19/0 to VLAN 300.

```
huawei(config)#vlan 300 smart
huawei(config)#port vlan 300 0/19 0
```


Copyright © Huawei Technologies Co., Ltd.

Create service flows. Set the service VLAN to 300, GEM port ID to 12, and user VLAN to 300, and use traffic profile **ftth_voip**.

```
huawei(config)#service-port vlan 300 gpon 0/1/0 ont 1 gemport 12 multi-service
 user-vlan 300 inbound traffic-table name ftth_voip outbound traffic-table name
ftth_voip
huawei(config)#service-port vlan 300 gpon 0/1/0 ont 2 gemport 12 multi-service
 user-vlan 300 inbound traffic-table name ftth_voip outbound traffic-table name
ftth_voip
```

Scenario 2:

Configure the mapping relationship between a GEM port and a VLAN. The service flow of user VLAN 3001 is mapped to GEM port 12 in the ONT line profile.

```
huawei(config)#ont-lineprofile gpon profile-name ftth
huawei(config-gpon-lineprofile-1)#gem mapping 12 2 vlan 3001
huawei(config-gpon-lineprofile-1)#commit
huawei(config-gpon-lineprofile-1)#quit
```

Create a service VLAN and add an upstream port to it. Add upstream port 0/19/0 to VLAN 300.

```
huawei(config)#vlan 300 smart
huawei(config)#vlan attrib 300 stacking
huawei(config)#port vlan 300 0/19 0
```

Create service flows. Set the service VLAN to 300, GEM port ID to 12, and user VLAN to 3001. Use traffic profile **ftth_voip**.

```
huawei(config)#service-port vlan 300 gpon 0/1/0 ont 1 gemport 12 multi-service
user-vlan 3001 tag-transform translate inbound traffic-table name ftth_voip
outboun
d traffic-table name ftth_voip
huawei(config)#service-port vlan 300 gpon 0/1/0 ont 2 gemport 12 multi-service
user-vlan 3001 tag-transform translate inbound traffic-table name ftth_voip
outboun
d traffic-table name ftth_voip
```

Step 9 Configure ONT voice service profiles.

ONT voice service profiles include the interface common profile, MGC interface profile, and POTS port profile.

- Interface common profile: saves common attributes of an ONT voice interface, including the fax mode, fax/modem negotiation mode, and priority of the coding and decoding mode.
- MGC interface profile: saves the IP address or domain name of the MGC, protocol port ID of the MGC transport layer to which the MG interface belongs, and DSCP priority of media packets.
- POTS port profile: saves physical attributes of a POTS port on an ONT, including the impedance, transmitting gain, receiving gain, and signaling type of the POTS port.

1. Configure an interface common profile.

   Run the **display ont-mg-attribute-profile** command to query the existing interface common profile in the system. If the existing interface common profile in the system does not meet the requirements, run the **ont-mg-attribute-profile add** command to add an interface common profile.

   In this example, the default interface common profile, namely interface common profile 1 is used.

2. Configure an MGC interface profile.

Copyright © Huawei Technologies Co., Ltd.

Run the **display ont-mgc-profile** command to query the existing MGC interface profile in the system. If the existing MGC interface profile in the system does not meet the requirements, run the **ont-mgc-profile add** command to add an MGC interface profile.

Create MGC interface profile 2, set the IP address of the MGC to 200.200.200.200, and use default values for other parameters.

```
huawei(config)#ont-mgc-profile add profile-id 2 primary-mgc 200.200.200.200
```

3. Configure a POTS port profile.

   Run the **display ont-pots-profile** command to query the existing POTS port profile in the system. If the existing POTS port profile in the system does not meet the requirements, run the **ont-pots-profile add** command to add a POTS port profile.

   In this example, the default POTS port profile, namely POTS port profile 1 is used.

Step 10 Configure the IP addresses of ONT H.248 users.

For ONT 1 and ONT 2, configure the IP address obtaining mode to the dhcp mode, set the management VLAN to VLAN 20, and use default values for other parameters.

```
huawei(config)#interface gpon 0/1
huawei(config-if-gpon-0/1)#ont ipconfig 0 1 dhcp vlan 20
huawei(config-if-gpon-0/1)#ont ipconfig 0 2 dhcp vlan 20
```

Step 11 Configure H.248 PSTN users.

1. Add an H.248 interface and apply an MGC interface profile to the interface.

   For ONT 1 and ONT 2, set the MG ID to 1, apply MGC interface profile 2 to ONT 1 and ONT 2, and use default values for other parameters.

   If parameters of an MGC interface profile are changed, the MGC interface profile must be reapplied to the ONT so that the changed parameters can take effect.

   ```
   huawei(config-if-gpon-0/1)#if-h248 add 0 1 1 mgc-profile profile-id 2
   huawei(config-if-gpon-0/1)#if-h248 add 0 2 1 mgc-profile profile-id 2
   ```

2. Add PSTN users.

   For ONT 1 and ONT 2, create a PSTN user, set the MG ID to 1 (identical to the MG ID of the H.248 interface), and set the physical terminal port ID to A0 and A1.

   ```
   huawei(config-if-gpon-0/1)#mgpstnuser add 0 1 1 mgid 1 terminalid A0
   huawei(config-if-gpon-0/1)#mgpstnuser add 0 2 1 mgid 1 terminalid A1
   ```

   Run the **display mgpstnuser attribute** command to check whether the configuration of the PSTN user is properly set.

   ```
   huawei(config-if-gpon-0/1)#display mgpstnuser attribute 0 1 1

   ---------------------------------------------------------------------------
     F/S/P                     : 0/1/0
     ONT ID                    : 1
     Port ID                   : 1

     MG ID                     : 1
     Terminal ID               : A0
   ...//The rest of the response information is omitted.

   huawei(config-if-gpon-0/1)#display mgpstnuser attribute 0 2 1

   ---------------------------------------------------------------------------
     F/S/P                     : 0/1/0
     ONT ID                    : 2
     Port ID                   : 1

     MG ID                     : 1
   ```


Copyright © Huawei Technologies Co., Ltd.

```
  Terminal ID                : A1
...//The rest of the response information is omitted.
```

Step 12 Apply ONT voice service profiles

After ONT voice service profiles are applied, if parameters in those profiles are changed, those profiles must be reapplied so that the changed parameters can take effect.

1. Apply an interface common profile.

   Run the **if-h248 attribute** command to apply an interface common profile to an H.248 interface or configure the interface customized parameters, or run the **ont-if-h248 bat-apply** command to bulk apply the interface common profiles to H.248 interfaces. If you use these two commands to apply the interface common profiles or configure the interface customized parameters repeatedly, the last configurations take effect.

   In this example, the default interface common profile, namely interface common profile 1 is used.

2. Apply a POTS port profile.

   Run the **pstnport electric** command to apply a POTS port profile to an H.248 interface or configure the interface customized parameters, or run the **ont-pstnport electric bat-apply** command to bulk apply the POTS port profiles to H.248 interfaces. If you use these two commands to apply the POTS port profiles or configure the interface customized parameters repeatedly, the last configurations take effect.

   In this example, the default POTS port profile, namely POTS port profile 1 is used.

Step 13 (Optional) Configure the H.248 user codec.

Run the **mgpstnuser codec** command to configure the H.248 user codec. The H.248 user codec will not be configured independently in this example.

Step 14 Configure the traffic profile for the IPTV service.

```
huawei(config)#traffic table ip index 8 cir off priority 4 priority-policy
local-setting
```

Step 15 Configure the VLAN translation policy and service port for the multicast service.

1. Configure the mapping relationship between a GEM port and an Ethernet port on the ONT.

   If the ONT is connected to the STB through Ethernet port 2, map the service flow of Ethernet port 2 to GEM port 13 in the ONT line profile.

   ```
   huawei(config)#ont-lineprofile gpon profile-name ftth
   huawei(config-gpon-lineprofile-1)#mapping mode port
   huawei(config-gpon-lineprofile-1)#gem mapping 13 1 eth 2
   huawei(config-gpon-lineprofile-1)#commit
   huawei(config-gpon-lineprofile-1)#quit
   ```

2. Configure the VLAN of the Ethernet port on the ONT.

   If the ONT is connected to the STB through Ethernet port 2, add Ethernet port 2 to VLAN 1000.

   ```
   huawei(config)#ont-srvprofile gpon profile-name ftth
   huawei(config-gpon-srvprofile-1)#port vlan eth 2 1000
   huawei(config-gpon-srvprofile-1)#multicast-forward untag
   huawei(config-gpon-srvprofile-1)#commit
   huawei(config-gpon-srvprofile-1)#quit
   ```

3. Create a service VLAN and add an upstream port to it.

   Add upstream port 0/19/0 to VLAN 1000.

Copyright © Huawei Technologies Co., Ltd.

```
huawei(config)#vlan 1000 smart
huawei(config)#port vlan 1000 0/19 0
```

4. Create service flows.

   Set the service VLAN to 1000, GEM port ID to 13, and user VLAN to 1000, and use traffic profile 8.

```
huawei(config)#service-port 1 vlan 1000 gpon 0/1/0 ont 1 gemport 13 multi-
service
 user-vlan 1000 rx-cttr 8 tx-cttr 8
huawei(config)#service-port 2 vlan 1000 gpon 0/1/0 ont 2 gemport 13 multi-
service
 user-vlan 1000 rx-cttr 8 tx-cttr 8
```

Step 16 Create an MVLAN and configure the IGMP version.

Set the IGMP version for the MVLAN to IGMP IPv6 v2.

```
huawei(config)#multicast-vlan 1000
huawei(config-mvlan1000)#igmp ipv6 version v2
  This operation will delete all IPv6 programs with source IP addresses in the
current multicast VLAN
  Are you sure to change current IGMP IPv6 version? (y/n)[n]:y
  Command is being executed. Please wait...
  Command has been executed successfully
```

Step 17 Configure a program library.

Set the mode for obtaining multicast programs to dynamic.

NOTE

You can set the mode for obtaining multicast programs to dynamic only when the IGMP mode is off.

```
huawei(config-mvlan1000)#igmp ipv6 mode off
  Are you sure to close IGMP IPv6? (y/n)[n]:y
  Command is being executed. Please wait...
  Command has been executed successfully

huawei(config-mvlan1000)#igmp ipv6 match mode disable
  Command has been executed successfully
```

(Optional) Set the address range for the dynamic programs. If you need to limit the address range of dynamic programs, perform this operation. For example, set the address range of dynamic programs to ff15::-ff15::ffff.

```
huawei(config-mvlan1000)#igmp ipv6 match group ipv6 ff15:: to-ipv6 ff15::ffff
```

Step 18 Set the IGMP IPv6 mode.

Select the IGMP IPv6 proxy mode.

```
huawei(config-mvlan1000)#igmp ipv6 mode proxy
  Are you sure to change IGMP IPv6 mode? (y/n)[n]:y
  Command is being executed. Please wait...
  Command has been executed successfully
```

Step 19 Configure the IGMP upstream port.

Set the IGMP upstream port ID to 0/19/0 and working mode to **default**. Protocol packets are transmitted to all the IGMP upstream ports in the multicast VLAN.

```
huawei(config-mvlan1000)#igmp uplink-port 0/19/0
huawei(config-mvlan1000)#btv
huawei(config-btv)#igmp uplink-port-mode default
Are you sure to change the uplink port mode?(y/n)[n]:y
```

Step 20 Configure multicast users.

Add service ports 1 and 2 as multicast users.

Copyright © Huawei Technologies Co., Ltd.

```
huawei(config-btv)#igmp policy service-port 1 normal
huawei(config-btv)#igmp policy service-port 2 normal
huawei(config-btv)#igmp user add service-port 1
huawei(config-btv)#igmp user add service-port 2
huawei(config-btv)#multicast-vlan 1000
huawei(config-mvlan1000)#igmp multicast-vlan member service-port 1
huawei(config-mvlan1000)#igmp multicast-vlan member service-port 2
huawei(config-mvlan1000)#quit
```

Step 21 Configure the VLAN translation policy and service port for the VoD service.

1. Configure the mapping relationship between a GEM port and a VLAN.

   The service flow of user VLAN 1100 is mapped to GEM port 13 in the ONT line profile.

   ```
   huawei(config)#ont-lineprofile gpon profile-name ftth
   huawei(config-gpon-lineprofile-1)#gem mapping 13 4 vlan 1100
   huawei(config-gpon-lineprofile-1)#commit
   huawei(config-gpon-lineprofile-1)#quit
   ```

2. Configure the VLAN of the Ethernet port on the ONT.

   If the ONT is connected to the STB through Ethernet port 2, add Ethernet port 2 to VLAN 1100.

   ```
   huawei(config)#ont-srvprofile gpon profile-name ftth
   huawei(config-gpon-srvprofile-1)#port vlan eth 2 1100
   huawei(config-gpon-srvprofile-1)#commit
   huawei(config-gpon-srvprofile-1)#quit
   ```

3. Create a service VLAN and add an upstream port to it.

   Add upstream port 0/19/0 to VLAN 1100.

   ```
   huawei(config)#vlan 1100 smart
   huawei(config)#port vlan 1100 0/19 0
   ```

4. Create service flows.

   Set the service VLAN to 1100, GEM port ID to 13, and VLAN translation mode to transparent transmission, and use traffic profile 8.

   ```
   huawei(config)#service-port 3 vlan 1100 gpon 0/1/0 ont 1 gemport 13
   rx-cttr 8 tx-cttr 8 tag-transform transparent
   huawei(config)#service-port 4 vlan 1100 gpon 0/1/0 ont 2 gemport 13
   rx-cttr 8 tx-cttr 8 tag-transform transparent
   ```

Step 22 (Optional) Configure the PITP function for PPPoE.

```
huawei(config)#raio-mode common pitp-pmode
huawei(config)#pitp enable pmode
```

Step 23 (Optional) Configure the DHCP option function for IPoE.

```
huawei(config)#raio-mode common dhcp-option82      //For DHCPv4 packets
huawei(config)#dhcp option82 enable                //For DHCPv4 packets
huawei(config)#raio-mode common dhcpv6-option      //For DHCPv6 packets
huawei(config)#dhcpv6 option enable                //For DHCPv6 packets
```

Step 24 Save the configuration on the OLT side.

```
huawei(config)#save
```

Step 25 Log in to the Web configuration window.

1. Configure the IP address of the PC network adapter to be in the same network segment with the IP address of the local maintenance Ethernet port on the ONT (default: 192.168.100.1).

Copyright © Huawei Technologies Co., Ltd.

2. Open the Web browser, and enter the IP address of the local maintenance Ethernet port on the ONT. In the login window, enter the user name (default: telecomadmin) and password (default: admintelecom) of the administrator. After the password is authenticated, the Web configuration window is displayed.

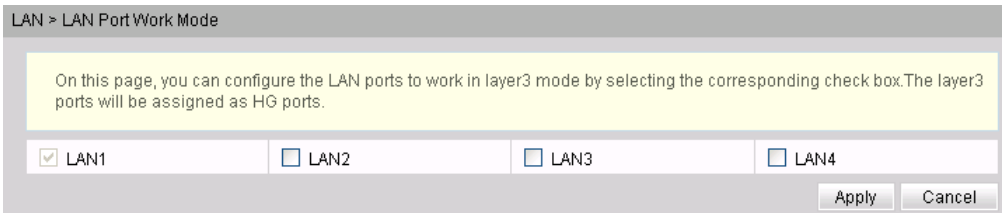
NOTE

The following steps are configured on the ONT through the web page.

Step 26 Configure the working mode for the LAN port.

1. Choose **LAN** > **LAN Port Work Mode** from the navigation tree. Select the check box next to LAN1 to set port LAN1 to work in Layer 3 mode. **Figure 19-8** shows the parameter settings.

Figure 19-8 Parameter settings on the Web page for the LAN port



2. Click **Apply** to make the configuration take effect.

Step 27 Configure parameters for a WAN interface.

1. Choose **WAN** > **WAN Configuration** from the navigation tree.
2. In the right pane, click **New**. In the dialog box that is displayed, set the parameters as follows:
   - Select **Enable WAN Connection** to enable the new WAN connection.
   - Set **Encapsulation Mode** to **PPPOE** or **IPOE** according to the IPv6 HSI solution.
   - Set **Protocol Type** to **IPv4/IPv6** (dual stack) or **IPv6** (DS-Lite).
   - Set **Mode** to **Route WAN**.
   - Set **Service List** to **INTERNET**.
   - Select **Enable VLAN**.
   - Set **VLAN ID** to **1001**.
   - Set **802.1p** to **0**.
   - Set **User Name** to **iadtest@pppoe** and **Password** to **iadtest**.
   - Select the check box next to **LAN1** in the **Binding options** area, indicating that the WAN port is bound to LAN1.

   IPv4 Information
   - Set **IP Acquisition Mode** to **PPPoE** when PPPoE is adopted for HSI. Set **IP Acquisition Mode** to **Static** or **DHCP** according to the data plan.
   - Select **Enable NAT** to enable the NAT function.

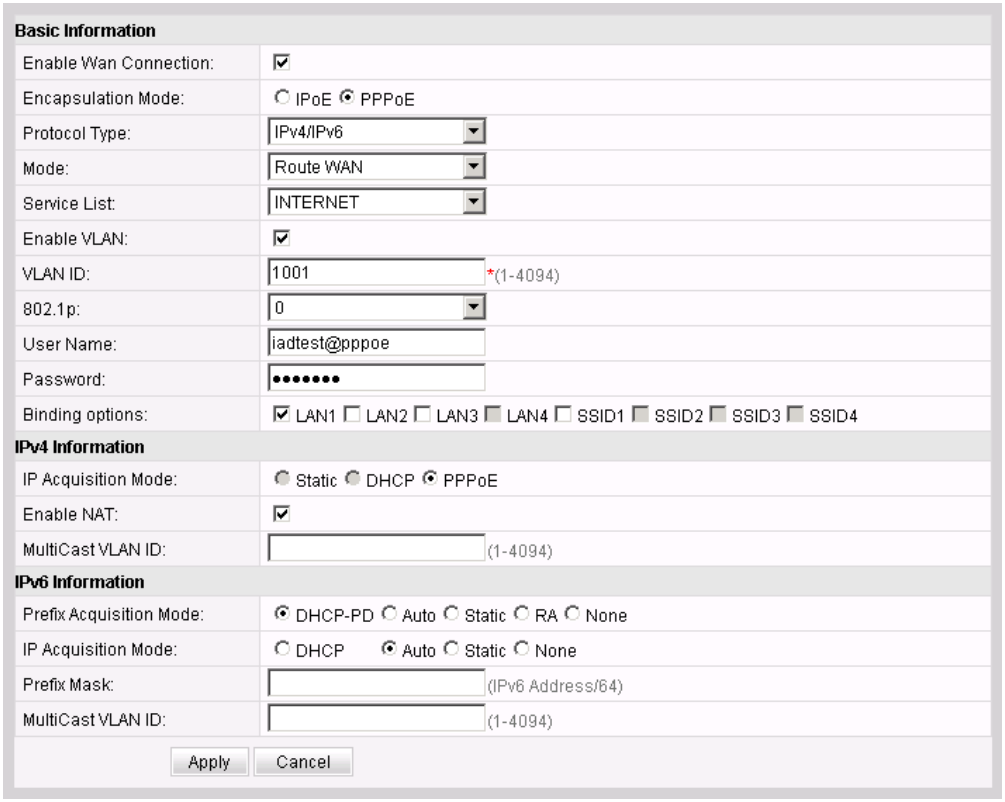
   IPv6 Information
   - **DHCP-PD** is recommended for **Prefix Acquisition Mode**.

Copyright © Huawei Technologies Co., Ltd.

- **DHCP** is recommended for **IP Acquisition Mode**.
- In case of DS-Lite solution and the **Protocol Type** in the **Basic Information** field is set to **IPv6**, set the **DSLite Work Mode** to **Auto**.

Figure 19-9 shows the parameter settings.

Figure 19-9 Parameter settings on the Web page for the WAN port



3. Click **Apply** to make the configuration take effect.

----End

Copyright © Huawei Technologies Co., Ltd.