



Dear Sir. / Madam,

How are you doing? Thanks for downloading this document.

Our company, ICI is an international telecommunication and ICT system consultant and value add distributor. We operate in Beijing, China. Our main business is selling fixed telecom network equipments to world-wide customers, e.g. telecom service providers and system integrators. We are specialized in below product series,

A. Optic transmission network equipments

- a) Huawei Metro 1000, OSN 1500, OSN 3500, and OSN 7500 SDH/MSTP equipments.
- b) Cisco 15454 / 15454E series SDH/MSTP equipments.
- c) Potevio and other major Chinese brands' microwave transmission equipments.

B. Data / IP network equipments

- a) Cisco routers
 - i. Cisco 1941/2901/2911/2921/2951/3925/3945 series ISR G2 access routers.
 - ii. Cisco ASR1000 / ASR9000 / CRS-1 series service provider core and edge routers.
- b) Cisco and Huawei Ethernet switches
 - i. Cisco 2960/2960S/3560/3560E/3560X/3750/3750E/3750X series access switches
 - ii. Cisco 4900/4500/6500 & Cisco Nexus 7000/5000/2000/1000 core and data center switches
 - iii. Huawei 2300/3300/5300/2700/3700/5700 series access switches.
 - iv. Huawei 9300/6700/7700 series high-end switches.

C. Access network equipments

- a) Huawei UA5000 and other integrated access equipments..
- b) Huawei MA5680T/MA5683T series OLT and FTTx equipments.
- c) Huawei MA5600 series MDU: MA5616 (ADSL2+&POTS), MA5620 (FE&POTS), MA5626 (POTS).

D. Other telecom project and system materials, e. g. fiber optic cables, CAT5E cables, and other bulk materials.

Our contact information and monthly-updated product catalog is as below,

Contact: **Morris Hagen**
Mobile: +86 1390 120 9254
Office Phone: +86 10 8893 7226
Email: morris@ici-cn.com
MSN Messenger: [zhzheng1982@hotmail.com](msn:zhzheng1982@hotmail.com)
Yahoo Messenger: morris.hagen@yahoo.com
Skype: morris.hagen.ici
Website: <http://www.ici-cn.com>

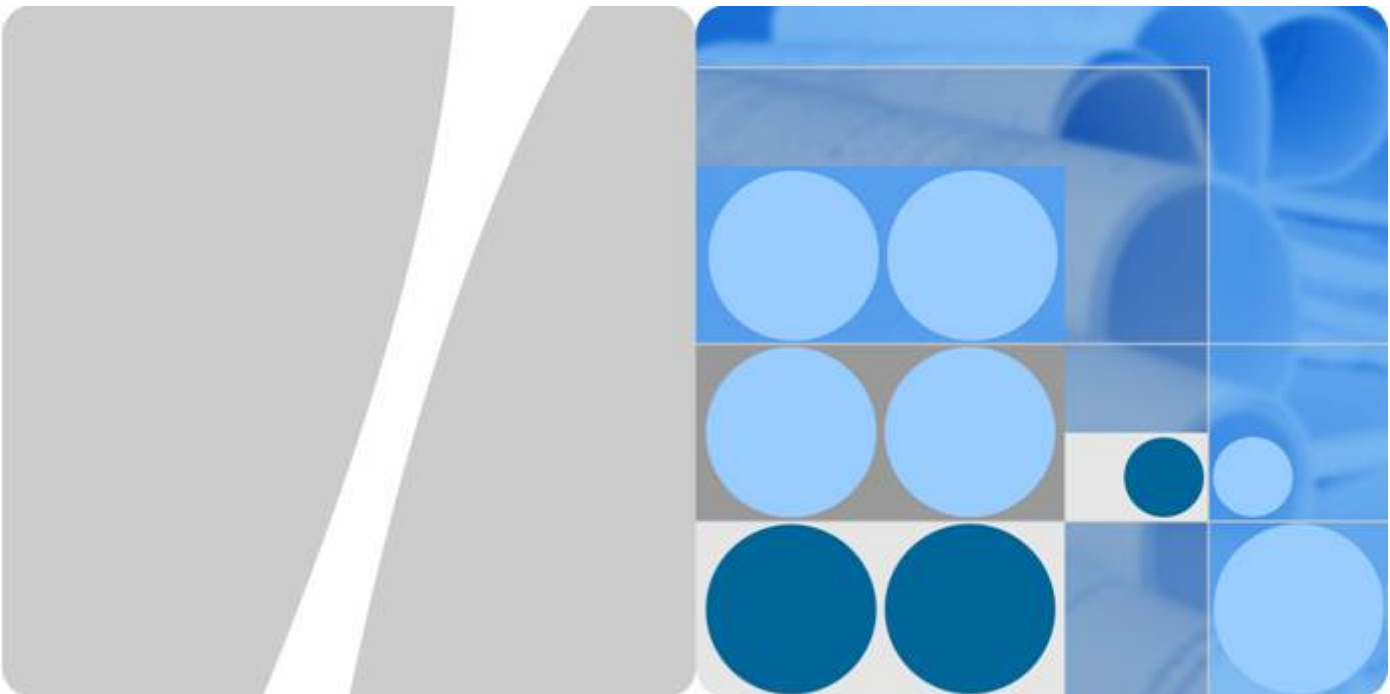
Monthly-updated Product Catalog: http://www.ici-cn.com/download/pricing/ICI_Catalog.xls

We sincerely wish that we could bring solid help to your business!

Best Regards,

Morris Hagen, Sales Team of [ICI](#)

Network Expertise Helps You Succeed



SingleFAN FTTx Solution

V100R007

Solution Configuration Guide

Issue 02

Date 2012-02-24

Copyright © Huawei Technologies Co., Ltd. 2012. 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



HUAWEI 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 the 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

About This Document

Product Version

The following table lists the product versions relevant to this document.

Product Name	Product Version
FTTx	V100R007
OLT	V800R010C00
MDU	V800R310
ONT	V200R005
U2000	V100R006C00

Intended Audience






This document mainly describes the characteristics, auxiliary devices, and networking, services and planning of sub-solutions of the FTTx solution.

The intended audience of this product description are as follows:

- Network planning engineers
- Installation and commissioning engineers
- Field maintenance engineers
- Network monitoring engineers
- System maintenance engineers
- Data configuration engineers

Symbol Conventions

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

Symbol	Description
 DANGER	Indicates a hazard with a high level of risk which, if not avoided, will result in death or serious injury.
 WARNING	Indicates a hazard with a medium or low level of risk which, if not avoided, could result in minor or moderate injury.
 CAUTION	Indicates a potentially hazardous situation which, if not avoided, could result in device damage, data loss, performance deterioration, or unexpected results.
 TIP	Indicates a tip that may help you solve a problem or save time.
 NOTE	Provides additional information to emphasize or supplement important points of the main text.

Change History

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

Updates in Issue 02 (2012-02-24)

Based on FTTx V100R007 issue 01 (2012-01-18), the document is updated as follows:

- Added the configurations of Type C single homing and Type C dual homing in [4.2 Configuring Base Station Access Network Protection](#).
- Added the scene of ONU dual GPON port independent upstream protection in [5.5 Configuration Example of Automatically Transmitting Site Information over Ethernet \(Independent Upstream Transmission\)](#).
- Added the scene of GPON Type C single homing protection in [5.3 Configuration Example of Automatically Transmitting Site Information over Ethernet \(Single Homing\)](#).

Updates in Issue 01 (2012-01-18)

The FTTx V100R007 is officially released for the first time. Based on FTTx V100R006 issue 02 (2011-09-15), the document is updated as follows:

- Optimized the FTTH and FTTB/C customer scenarios.

Contents

About This Document.....	ii
1 Configuring the FTTH Service.....	1
1.1 FTTH Data Plan.....	1
1.1.1 Security Design.....	1
1.1.2 Device Management Data Plan.....	6
1.1.3 Internet Access Service Data Plan.....	8
1.1.4 Voice Service Data Plan.....	10
1.1.5 IPTV Service Data Plan.....	13
1.2 GPON Access: Configuring FTTH Service.....	15
1.2.1 Reference of GPON ONT Capability Sets.....	15
1.2.2 Bridging ONT Network Scenario.....	20
1.2.3 Gateway ONT Network Scenario.....	70
1.2.4 Configuring FTTH Triple Play Service in Simplified Mode.....	109
2 Configuring the FTTB and FTTC Services.....	117
2.1 FTTB and FTTC Service Overview.....	117
2.1.1 Basic Concept.....	117
2.1.2 Scenario and Hardware Configuration.....	119
2.1.3 GPON ONU Capability Sets.....	121
2.2 FTTB and FTTC Data Plan.....	124
2.2.1 Security Design.....	124
2.2.2 Device Management Data Plan.....	129
2.2.3 QoS Plan.....	130
2.2.4 Internet Access Service Data Plan.....	133
2.2.5 VoIP Service Data Plan.....	135
2.2.6 IPTV Service Data Plan.....	138
2.3 Configuring FTTB/FTTC Services in Various Scenarios.....	141
2.3.1 FTTB Networking (LAN Access Without HGW).....	142
2.3.2 FTTB/C Scenario (xDSL Access, Without HGW).....	164
2.3.3 FTTB+HGW Scenario (Voice Service Provided by ONU).....	186
2.3.4 FTTB+HGW Networking (HGW Providing the VoIP Service).....	219
3 Configuring the FTTO Service.....	251
3.1 Configuring the TDM PBX Access Service (SDH-based).....	252

3.2 Configuring the Enterprise Router Access Service.....	252
3.3 Configuring the IP PBX Access Service.....	260
3.4 Configuring the POTS Access Service of the Enterprise.....	261
4 Configuring the Base station access Service.....	270
4.1 Configuring Base station access Clock Synchronization.....	271
4.1.1 Overview of Base station access Clock Synchronization.....	271
4.1.2 Configuring BITS Clock Synchronization.....	275
4.1.3 Configuring E1/STM-1 Line Clock Synchronization.....	278
4.1.4 Configuring Ethernet Clock Synchronization.....	281
4.2 Configuring Base Station Access Network Protection.....	284
4.3 Configuring the Native TDM Base station access Service (SDH-based, MA5628).....	289
4.4 Configuring the Native TDM Base station access Service (SDH-based, OT928G).....	297
4.5 Configuring the QinQ Private Line Base station access Service for the OLT.....	304
5 Configuring the FTTx Electric Power Applications.....	313
5.1 Configuration Example of Transmitting Video Monitoring Data by Using the Ethernet Access.....	315
5.2 Configuration Example of Intelligently Collecting Power Consumption Information by Using the Ethernet Access.....	323
5.3 Configuration Example of Automatically Transmitting Site Information over Ethernet (Single Homing).....	332
5.4 Configuration Example of Automatically Transmitting Site Information over Ethernet (Dual Homing).....	347
5.5 Configuration Example of Automatically Transmitting Site Information over Ethernet (Independent Upstream Transmission).....	363
5.6 Configuration Example of Transmitting Information Collected in Centralized Mode in the Smart Grid over a Serial Port.....	383
6 Configuring Example of EoC Broadband Services.....	395

1 Configuring the FTTH Service

1.1 FTTH Data Plan

1.1.1 Security Design

Security design involves designs for system security, user security, and service security. 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	Suggestion	Configuration Method
DoS attack	Enable the anti-DoS-attack function.	After the anti-DoS-attack function is enabled, control packets are monitored and those exceeding the number threshold are discarded.	Use this solution in a new deployment.	<ol style="list-style-type: none"> 1. Run the security anti-dos enable command to enable global anti-DoS attack. 2. Run the security anti-dos control-packet policy command to configure the policy of processing protocol packets when a DoS attack occurs. 3. Run the security anti-dos control-packet rate command to configure the threshold of the rate for sending protocol packets to the CPU.
ICMP attack	Enable the anti-ICMP-attack function.	After the anti-ICMP-attack function is enabled, a device discards the ICMP 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 in a new deployment.	Run the security anti-icmpattack enable command to enable anti-ICMP attack.

Security Vulnerability	Solution	Description	Suggestion	Configuration Method
IP attack	Enable the anti-IP-attack function.	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 in a new deployment.	Run the security anti-ipattack enable command to enable anti-IP attack.

User Security

Security Vulnerability	Solution	Description	Suggestion	Configuration Method
MAC spoofing	Enable the anti-MAC-duplicate function.	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 in a new deployment.	Run the security anti-macduplicate enable command to enable anti-MAC-duplicate.

Security Vulnerability	Solution	Description	Suggestion	Configuration Method
IP spoofing	Enable the anti-IP spoofing function.	After the anti-IP spoofing is enabled, it can prevent users from forging IP addresses to perform malicious attacks.	Use this solution in a new deployment.	<p>The anti-IP spoofing function can be enabled or disabled at three levels. This anti-IP spoofing function takes effect only when it is enabled at all three levels.</p> <ol style="list-style-type: none"> 1. Global level: Run the security anti-ipspoofing enable command in global configuration mode. 2. VLAN level: Run the security anti-ipspoofing enable command in VLAN service profile configuration mode. 3. Service port level: Run the security anti-ipspoofing service-port <i>serviceport-id</i> enable command.

Service Security

Security Vulnerability	Solution	Description	Suggestion	Configuration Method
Unauthorized broadband access of small enterprises (IPoE)	DHCP option 82 is enabled on the access network, and the BRAS implements user authentication based on the RAIO information.	<p>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:</p> <ul style="list-style-type: none"> ● 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.	<p>The DHCP option 82 function can be enabled or disabled at four levels. The DHCP option 82 function takes effect only when it is enabled at all four levels.</p> <ol style="list-style-type: none"> 1. Global level: Run the dhcp option82 enable command in global configuration mode. 2. Port level: Run the dhcp option82 port or dhcp option82 board command to enable the function at the port level. 3. VLAN level: Run the dhcp option82 enable command in VLAN service profile configuration mode. 4. Service port level: Run the dhcp option82 service-port command.

Security Vulnerability	Solution	Description	Suggestion	Configuration Method
Broadband access of residential users (PPPoE), user account theft/borrowing	PPPoE+ (PITP) is enabled on the access network and the BRAS implements user authentication based on binding of RAIO 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: <ul style="list-style-type: none"> ● 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.	The PITP function can be enabled or disabled at four levels. The PITP function takes effect only when it is enabled at all four levels. <ol style="list-style-type: none"> 1. Global level: Run the pitp enable pmode command in global configuration mode. 2. Port level: Run the pitp port or pitp board command to enable the function at the port level. 3. VLAN level: Run the pitp enable command in VLAN service profile configuration mode. 4. Service port level: Run the pitp service-port command.

1.1.2 Device Management Data Plan

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.

Plan	Device/Service	Description
	Home gateway (HG)	Use a single-tagged S-VLAN as the management VLAN of the HG that are managed by the ITMS. 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 HG 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 (a bridging ONT)	Internet access service	The PC obtains a public network IP address using PPPoE dialup for Internet access. The ONT is only used for transparent transmission.
	IPTV service	Through DHCP, the STB obtains a public network IP address and the subscriber can order programs. The ONT is only used for transparent transmission.
	VoIP service	The ONT, functioning as a DHCP client, obtains the IP address through DHCP, or the NMS allocates a static IP address to the ONT through the configuration file. The voice signaling streams and the media streams of multiple POTS ports share an IP address. Media streams can be distinguished by different ports.
IP address plan (a gateway ONT)	Internet access service	The ONT, functioning as a PPPoE client, obtains a public network IP address through the PPPoE dialup. Meanwhile, the ONT, functioning as a DHCP server, allocates private network IP addresses to PCs that access the Internet through the network cables or WiFi. After the network address translation (NAT), PCs of the private network share a public network IP address.
	IPTV service	The ONT, functioning as a DHCP client, obtains a public network IP address through DHCP. Meanwhile, the ONT, functioning as a DHCP server, allocates private network IP addresses to STBs. After NAT, STBs of the private network share an IP address.
	VoIP service	The ONT, functioning as a DHCP client, obtains the IP address through DHCP, or the NMS allocates a static IP address to the ONT through the configuration file. The voice signaling streams and the media streams of multiple POTS ports share an IP address. Media streams can be distinguished by different ports.

Plan	Device/Service	Description
	TR069 management	In TR069-based management, maintenance and service provisioning, the ONT, functioning as a DHCP client, obtains a public network IP address through DHCP and connects to the TR069 server (ACS).

1.1.3 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 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 translates the C-VLAN to S-VLAN+C-VLAN.
	Double-tagged VLAN	ONT: The ONT transmits all packets transparently and does not add the VLAN tag to packets. OLT: The OLT adds double-tagged VLAN (S+C) to packets.
Bridging ONT + HG	Double-tagged VLAN	The upstream packets sent from the HG carry user-VLANs and the ONT transparently transmits them. OLT: The OLT translates the U-VLAN to S-VLAN+C-VLAN.
	Double-tagged VLAN	The upstream packets sent from the HG do not carry any VLAN tag and the ONT transparently transmits them. OLT: The OLT adds the double-tagged VLAN to packets and translates ONTID +Untag VLAN to S-VLAN+C-VLAN.

Application Scenario	VLAN Plan	VLAN Translation Policy
Gateway ONT	Double-tagged VLAN	<p>ONT: Configure the VLAN through iTMS or adopt the factory default settings. All packets do not carry any VLAN tag.</p> <p>OLT: The upstream packets sent from HG do not carry any VLAN tag. The OLT translates the untagged VLAN to S-VLAN+C-VLAN.</p>
	Double-tagged VLAN	<p>ONT: Configure the VLAN through iTMS or adopt the factory default settings. Packets carry C-VLAN tags.</p> <p>OLT: The upstream packets sent from HG carry CVLAN tags. The OLT translates C-VLAN to S-VLAN+C'-VLAN.</p>

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 ONT/ONU/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.

1.1.4 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.

VLAN and VLAN Translation Policy.

Application Scenario	VLAN Plan	VLAN Translation Policy
Bridging ONT	Single-tagged VLAN	ONT: ONTs provide the VoIP service and use the same S-VLAN.
	Double-tagged VLAN	ONT: ONTs 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 ONT + HG	Single-tagged VLAN	ONT: The upstream packets sent from the HG carry user-VLANs and the ONT transparently transmits them. OLT: The OLT translates user-VLAN to S-VLAN.
	Double-tagged VLAN	ONT: The upstream packets sent from the HG carry user-VLANs and the ONT transparently transmits them. OLT: OLT: The OLT translates user-VLAN to S-VLAN+C-VLAN.
Gateway ONT	Single-tagged VLAN	ONT: Configure the VLAN of the WAN port of VoIP service through iTMS or adopt the factory default settings. OLT: The OLT transparently transmits all VLANs (the C-VLAN is the same as the planned S-VLAN).
	Single-tagged VLAN	ONT: Configure the VLAN of the WAN port of VoIP service through iTMS or adopt the factory default settings. OLT: The OLT translates C-VLAN to S-VLAN (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 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 ONT/ONU/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 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 VoIP service
		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	-	
	Signaling port ID	Choose the transmission method 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)		

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 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 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: <ul style="list-style-type: none"> ● 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: <ul style="list-style-type: none"> ● DEL: direct exchange lines (default) ● ECPBX: earth calling PBX ● LCPBX: loop calling PBX ● PayPhone: pay phone

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.
	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 need not be modified if there is no special requirement.
	Ring 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.

1.1.5 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 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.

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 + HG	Multicast service	Single-tagged VLAN	ONTs transparently transmit upstream packets with M-VLANs sent from HG. 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 HG 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 HG. The OLT implements VLAN translation: U->S.
		Double-tagged VLAN	ONTs transparently transmit the upstream U-VLANs sent from HG. 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.

- 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 ONT/ONU/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.

1.2 GPON Access: Configuring FTTH Service

This topic describes how to configure the Internet access service, voice service and multicast service in GPON access mode in FTTH network scenario.

Context

The description of this topic is based on the mode below. You can query the current mode in the diagnosis mode.

Mode	Query Methods
GPON profile mode	<pre> huawei (config) #diagnose huawei (diagnose) %%display xpon mode ----- Current config mode: Profile-mode ----- </pre>

1.2.1 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.

ONU Capability Sets

Table 1-1 shows the ONT capability sets provided by Huawei.

Table 1-1 List of ONT capability sets

ONT Type	Number of Ports	Number of GEM Ports	IP Addresses 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
HG810	1 ETH	32	Not supported	8	VLAN/ PRI/ VLAN + PRI	PQ/GEM port CAR	T-CONT 0:3 T-CONT 1-7:4
HG810a	1 ETH	32	Not supported	8	VLAN/ PRI/ VLAN + PRI	PQ/GEM port CAR	T-CONT 0:3 T-CONT 1-7:4
HG8010	1 ETH	32	Supported	8	VLAN/ PRI/ VLAN + PRI/ IPTOS/ Port/ Port + VLAN/ Port + PRI/Port + VLAN + PRI	PQ/Gem port CAR/ Flow CAR	T-CONT 0:3 T-CONT 1-7:4
HG810	1 ETH + 1 POTS	32	Supported	8	VLAN/ PRI/ VLAN + PRI/ IPTOS/ Port/ Port + VLAN/ Port + PRI/Port + VLAN + PRI	PQ/Gem port CAR/ Flow CAR	T-CONT 0:3 T-CONT 1-7:4
HG813	4 ETH	32	Not supported	8	VLAN/ PRI/ VLAN + PRI/ IPTOS/ Port	PQ/Gem port CAR/ Flow CAR	T-CONT 0:3 T-CONT 1-7:4

ONT Type	Number of Ports	Number of GEM Ports	IP Addresses 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
HG8120	2 ETH + 1 POTS	32	Supported	8	VLAN/ PRI/ VLAN + PRI/ IPTOS/ Port/ Port + VLAN/ Port + PRI/Port + VLAN + PRI	PQ/Gem port CAR/ Flow CAR	T-CONT 0:3 T-CONT 1-7:4
HG8120R	2 ETH + 1 POTS	32	Supported	8	VLAN/ PRI/ VLAN + PRI/ IPTOS/ Port/ Port + VLAN/ Port + PRI/Port + VLAN + PRI	PQ/Gem port CAR/ Flow CAR	T-CONT 0:3 T-CONT 1-7:4
HG850	4 ETH + 2 POTS	32	Supported	8	VLAN/ PRI/ VLAN + PRI	PQ/ Gemport CAR	T-CONT 0:3 T-CONT 1-7:4
HG8500	4 ETH + 2 POTS	8	Supported	8	VLAN/ PRI/ VLAN + PRI/Port	PQ/GEM port CAR	T-CONT 0-7:8
HG850a	4 ETH + 2 POTS	32	Supported	8	VLAN/ PRI/ VLAN + PRI/ IPTOS/ Port	PQ/Gem port CAR/ Flow CAR	T-CONT 0:3 T-CONT 1-7:4

ONT Type	Number of Ports	Number of GEM Ports	IP Addresses 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
HG851	4 ETH + 2 POTS	32	Supported	8	VLAN	Gem port CAR	T-CONT 0:3 T-CONT 1-7:4
HG851a	4 ETH + 2 POTS	32	Supported	8	VLAN/ PRI/ VLAN + PRI/ IPTOS/ Port	PQ/Gem port CAR/ Flow CAR	T-CONT 0:3 T-CONT 1-7:4
HG860	1 ETH + 1 CATV	32	Not supported	8	VLAN/ PRI/ VLAN + PRI/ IPTOS/ Port	PQ/Gem port CAR/ Flow CAR	T-CONT 0:3 T-CONT 1-7:4
HG861	1 ETH + 1 CATV	32	Not supported	8	VLAN/ PRI/ VLAN + PRI/ IPTOS/ Port	PQ/Gem port CAR/ Flow CAR	T-CONT 0:3 T-CONT 1-7:4
HG863	4 ETH	32	Not supported	8	VLAN/ PRI/ VLAN + PRI/ IPTOS/ Port/ Port + VLAN/ Port + PRI/Port + VLAN + PRI	PQ/Gem port CAR/ Flow CAR	T-CONT 0:3 T-CONT 1-7:4
HG865	4 ETH + 4 POTS + 1 CATV	32	Supported	8	VLAN/ PRI/ VLAN + PRI	PQ/GEM port CAR	T-CONT 0:3 T-CONT 1-7:4

ONT Type	Number of Ports	Number of GEM Ports	IP Addresses 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
HG866	4 ETH + 2 POTS	8	Supported	8	VLAN/ PRI/ VLAN + PRI/Port	PQ/GEM port CAR	T-CONT 0-7:8
HG8240/ HG8240B/ HG8240R	4 ETH + 2 POTS	32	Supported	8	VLAN/ PRI/ VLAN + PRI/ IPTOS/ Port/ Port + VLAN/ Port + PRI/Port + VLAN + PRI	PQ/Gem port CAR/ Flow CAR	T-CONT 0:3 T-CONT 1-7:4
HG8245/ HG8245R/ HG8245T	4 ETH + 2 POTS	32	Supported	8	VLAN/ PRI/ VLAN + PRI/ IPTOS/ Port/ Port + VLAN/ Port + PRI/Port + VLAN + PRI	PQ/Gem port CAR/ Flow CAR	T-CONT 0:3 T-CONT 1-7:4
HG8242	4 ETH + 2 POTS + 1 CATV	32	Supported	8	VLAN/ PRI/ VLAN + PRI/ IPTOS/ Port/ Port + VLAN/ Port + PRI/Port + VLAN + PRI	PQ/Gem port CAR/ Flow CAR	T-CONT 0:3 T-CONT 1-7:4

ONT Type	Number of Ports	Number of GEM Ports	IP Addresses 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/ HG8247T	4 ETH + 2 POTS + 1 CATV	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

- Bridging ONTs: HG8010, HG8110, HG8120, HG8240, HG8240B and HG8242
- Gateway ONTs: HG8120R, HG8240R, HG8245, HG8245R, HG8245T, HG8247 and HG8247T

1.2.2 Bridging ONT Network Scenario

This topic describes how to configure Internet access services, voice services, and video services when bridging ONTs are used to build an FTTH network.

Service Requirements and Application Scenario

When bridging ONTs are used to build an FTTH network, there are two application scenarios: bridging ONT scenario and bridging ONT + HG 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

Figure 1-1 Bridging ONT

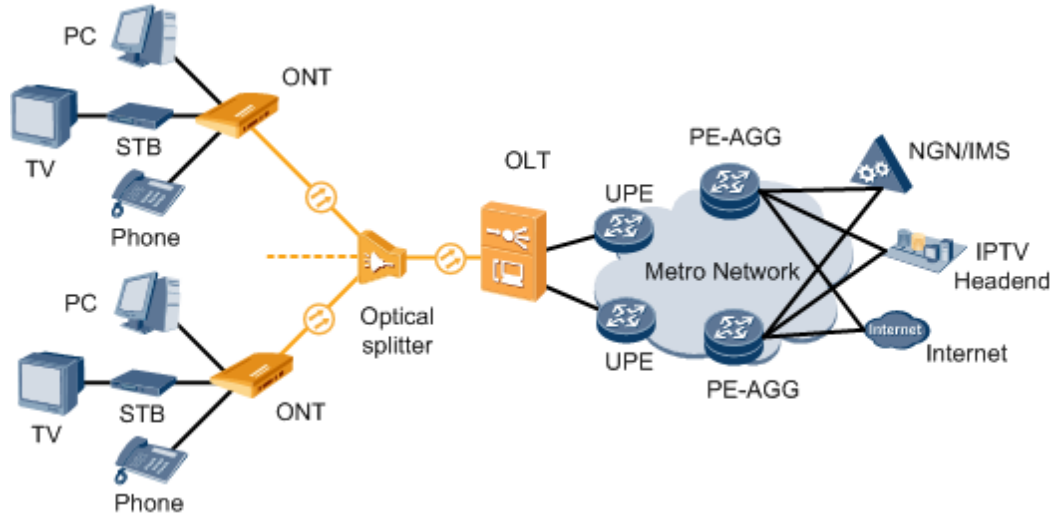
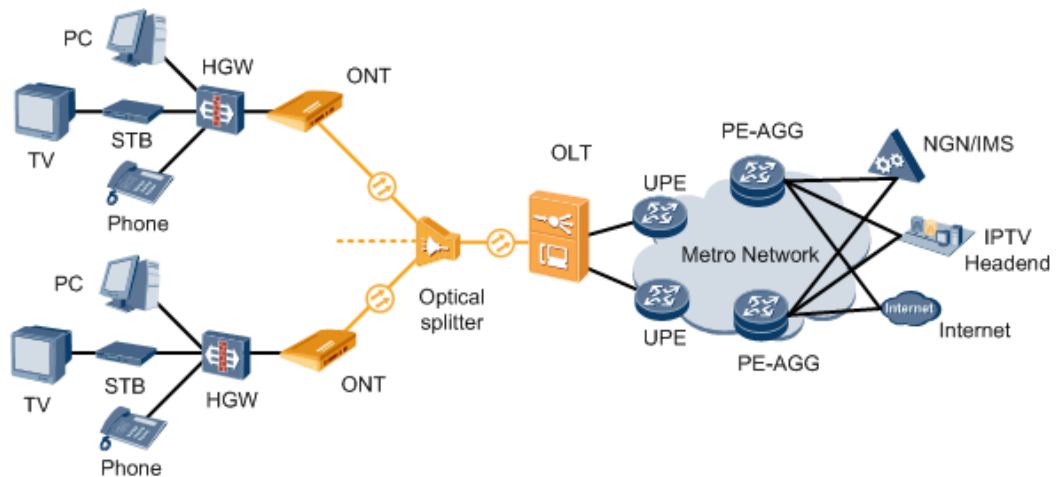


Figure 1-2 Bridging ONT + HG



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 1-2 Data plan

Item	Data
DBA profile	Profile name: fthfth_dba Profile type: type3 Assured bandwidth: 8 Mbit/s Maximum bandwidth: 20 Mbit/s
ONT line profile	Profile name: fth 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: fth 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.

Create the same DBA profile for different types of services. Set the profile name to **fthfth_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**

- 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.
- 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.
- 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
-----
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.

 **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.

---End

Configuring the Layer 2 Internet Access Service

The OLT is connected to the remote ONT 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 ONT has been added to the OLT. For details, see [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

Table 1-3 Data plan

Item	Data
ONT line profile	Profile name: ftth T-CONT ID: 4 GEM port ID for Internet access service: 14
ONT service profile	Profile name: ftth ONT port capability set: adaptive

Item	Data
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

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. Perform this step in the **bridging ONT (double-tagged VLAN)** scenario.

Table 1-4 Scenario plan

Scenario	VLAN Plan	VLAN Translation Policy
Scenario 1	Double-tagged VLAN <ul style="list-style-type: none"> ● 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	VLAN Plan	VLAN Translation Policy
Scenario 2	Double-tagged VLAN <ul style="list-style-type: none"> ● 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.

```
huawei (config) #service-port vlan 100 gpon 0/1/0 ont 1 gempport 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 gempport 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 fthh
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 fthh
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 fthh_hsi.

```
huawei(config)#service-port vlan 100 gpon 0/1/0 ont 1 gempport 14 multi-
service
user-vlan untagged tag-transform add-double inner-vlan 1001 inbound
traffic-table
name fthh_hsi outbound traffic-table name fthh_hsi
huawei(config)#service-port vlan 100 gpon 0/1/0 ont 2 gempport 14 multi-
service
user-vlan untagged tag-transform add-double inner-vlan 1002 inbound
traffic-table
name fthh_hsi outbound traffic-table name fthh_hsi
```

3. Perform this step in the **bridging ONT + HG (double-tagged VLAN)** scenario.

Table 1-5 Scenario plan

Scenario	VLAN Plan	VLAN Translation Policy
Scenario 1	Double-tagged VLAN <ul style="list-style-type: none"> ● S-VLAN ID: 100 ● S-VLAN type: smart ● S-VLAN attribute: stacking ● C-VLAN ID: 1001-1002 ● U-VLAN ID: 45 	The upstream packets sent from the HG carry user-VLANs and the ONT transparently transmits them. OLT: The OLT performs VLAN translation: U<->S+C. The C-VLAN of every ONT differs from each other.

Scenario	VLAN Plan	VLAN Translation Policy
Scenario 2	Double-tagged VLAN <ul style="list-style-type: none"> ● SVLAN: 100 ● SVLAN type: smart ● SVLAN attribute: stacking ● CVLAN ID: 1001-1002 ● ULAN: untagged 	The upstream packets sent from the HG do not carry any VLAN tag and the ONT transparently transmits them. OLT: The OLT adds two VLAN tags (S+C) to the 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 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 HG to ONT, namely, U-VLAN.

```
huawei(config)#ont-lineprofile gpon profile-name ftth
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 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
```

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 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
```

– 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 HG 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 gempport 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 gempport 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
```

4. Save the data.

```
huawei(config)#save
```

- Configure the ONT.

The Layer 2 Internet access service requires no configuration on the ONT.

----End

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.

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 ONT has been added to the OLT. For details, see [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

Table 1-6 Data Plan

Item	Data
ONT line profile	Profile name: fthh T-CONT ID: 4 GEM port ID: 12
ONT service profile	Profile name: fthh ONT 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.

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 **fthh_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 fthh_voip cir off priority 5 priority-policy local-setting
```

2. Perform this step in the **bridging ONT (single VLAN tag)** scenario.

Table 1-7 Data plan

Scenario	VLAN Plan	VLAN Translation Policy
Bridging ONT	Single VLAN tag <ul style="list-style-type: none">● VLAN ID: 300● VLAN type: smart● VLAN attribute: common	ONT: provides the VoIP service and uses the same SVLAN.

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 fthh
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
```

3. Perform this step in the **bridging ONT (double VLAN tags)** scenario.

Table 1-8 Data plan

Scenario	VLAN Plan	VLAN Translation Policy
Bridging ONT	Double VLAN tags <ul style="list-style-type: none"> ● 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
outbound 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
```

```
outbound
d traffic-table name ftth_voip
```

4. Perform this step in the **bridging ONT+HGW (single VLAN tag)** scenario.

Table 1-9 Data plan

Scenario	VLAN Plan	VLAN Translation Policy
Bridging ONT +HG	Single VLAN tag <ul style="list-style-type: none"> ● VLAN ID: 300 ● VLAN type: smart ● VLAN attribute: common ● UVLAN ID: 45 	ONT: Upstream packets of the HGW carry the user VLAN and the ONT transparently transmits the packets. OLT: implements VLAN translation: U<->S.

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 ONT line profile.

 **NOTE**

The user VLAN is the VLAN in the packets sent from the HG 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 45
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 HG through Ethernet port 1, 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
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 45, and use traffic profile **ftth_voip**.

```
huawei(config)#service-port vlan 300 gpon 0/1/0 ont 1 gempport 12 multi-
service
user-vlan 45 inbound traffic-table name ftth_voip outbound traffic-table
name
ftth_voip
huawei(config)#service-port vlan 300 gpon 0/1/0 ont 2 gempport 12 multi-
service
user-vlan 45 inbound traffic-table name ftth_voip outbound traffic-table
name
ftth_voip
```

5. Perform this step in the **bridging ONT+HGW (double VLAN tags)** scenario.

Table 1-10 Data plan

Scenario	VLAN Plan	VLAN Translation Policy
Bridging ONT +HG	Double VLAN tags <ul style="list-style-type: none"> ● SVLAN ID: 300 ● SVLAN type: smart ● SVLAN attribute: stacking ● UVLAN ID: 45 ● CVLAN ID: 3001 	ONT: Upstream packets of the HGW carry the user VLAN and the ONT transparently transmits the packets. OLT: implements VLAN translation: U<->S+C.

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 ONT line profile.

 **NOTE**

The user VLAN is the VLAN in the packets sent from the HG 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 45
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 HG through Ethernet port 1, 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
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)#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, user VLAN to 45, and CVLAN to 3001. Use traffic profile **ftth_voip**.

```

huawei(config)#service-port vlan 300 gpon 0/1/0 ont 1 gempport 12 multi-
service
user-vlan 45 tag-transform translate-and-add inner-vlan 3001 inbound
traffic-table
name ftth_voip outbound traffic-table name ftth_voip
huawei(config)#service-port vlan 300 gpon 0/1/0 ont 2 gempport 12 multi-
service
user-vlan 45 tag-transform translate-and-add inner-vlan 3001 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 ONT 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 with the IP address of the local maintenance Ethernet port on the ONT (default: 192.168.100.1).
- b. 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.

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 1-3 shows the parameter settings.

Figure 1-3 Parameter settings on the Web page for the voice WAN interface

		New	Delete
	Connection Name	VLAN/Priority	Protocol Type
<input type="checkbox"/>	1_VOIP_R_VID_1001	1001/0	IPv4

Basic Information			
Enable Wan Connection:	<input checked="" type="checkbox"/>		
Encapsulation Mode:	<input checked="" type="radio"/> IPoE <input type="radio"/> PPPoE		
Protocol Type:	IPv4		
Mode:	Route WAN		
Service List:	VOIP		
Enable VLAN:	<input checked="" type="checkbox"/>		
VLAN ID:	300 <small>*(1-4094)</small>		
802.1p:	5		
IP Acquisition Mode:	<input type="radio"/> Static <input checked="" type="radio"/> DHCP <input type="radio"/> PPPoE		
Vendor ID:	<input type="text"/> <small>(The vendor ID must be 0 - 63 characters in length.)</small>		
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>			

- c. Click **Apply**.
3. Configure parameters for the H.248-based voice interface.
 - a. Choose **Voice > VoIP Basic Configuration**.
 - b. In the right pane, configure the parameters as follows:
 - Set **Primary MGC Address** to **200.200.200.200**.
 - Set **MID Format** to **DomainName** and **MG Domain** to **huawei.com**.
 - Set **Signaling Port** to **1_VOIP_R_VID_300**.
 - Set **Region** to **CN-China**.

Figure 1-4 shows the parameter settings.

Figure 1-4 Parameter settings on the Web page for the H.248-based voice interface

Interface Basic Parameters		
On this page, you can set the basic parameters for the voice interface.		
Primary MGC Address:	<input type="text" value="200.200.200.200"/>	*(IP or Domain)
Primary MGC Port:	<input type="text" value="2944"/>	*(0-65535)
Standby MGC Address:	<input type="text"/>	(IP or Domain)
Standby MGC Port:	<input type="text" value="2944"/>	(0-65535)
MG Domain:	<input type="text" value="huawei.com"/>	
Local Port:	<input type="text" value="2944"/>	*(0-65535)
Device Name:	<input type="text"/>	
MID Format:	<input type="text" value="DomainName"/>	
Digitmap Match Mode:	<input type="text" value="Min"/>	
Digitmap Auto Match Enable:	<input type="checkbox"/>	
RTP TID Prefix:	<input type="text" value="0"/>	
Start Number of RTP TID:	<input type="text" value="0"/>	
Width of RTP TID Number:	<input type="text" value="6"/>	
Signaling Port:	<input type="text" value="2_VOIP_R_VID_300"/>	(Select the name of the WAN that w messages.)
Media Port:	<input type="text"/>	(Select the name of the WAN that w media port name is same with signaling port name when it is
Region:	<input type="text" value="CN - China"/>	
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>		

- c. Click **Apply**.
4. Configure parameters for H.248-based voice users.

- a. Choose **Voice > VoIP Basic Configuration**.
- b. In the right pane, click **New**. In the dialog box that is displayed, set the parameters for user 1 as follows:
 - Select **Enable Line Name**.
 - Set **Line Name** to **A0**.
 - Set **Associated POTS** to **1**.
 - Click **Apply**.

In the right pane, click **New** to add voice user 2, and set the parameters for voice user 2 as follows:

- Select **Enable Line Name**.
- Set **Line Name** to **A1**.
- Set **Associated POTS** to **2**.
- Click **Apply**.

Figure 1-5 shows the parameter settings.

Figure 1-5 Parameter settings on the Web page for H.248-based voice users

User Basic Parameters

On this page, you can set the basic parameters for the voice users.

	Sequence	Line Name	Associated POTS
<input type="checkbox"/>	1	A0	1
<input type="checkbox"/>	2	A1	2

Enable Line Name:

Line Name:

Associated POTS:

- c. Click **Apply**.
5. (Optional) Configure routes.

You need to configure routes when the IP address of the ONT and that of the voice server are in different network segments.

 - a. Choose **Route > Default Route Configuration**.
 - b. Select **Enable Default Route** and set **WAN Name** to **1_VOIP_R_VID_300**.

Figure 1-6 shows the parameter settings.

Figure 1-6 Route parameter settings

- c. Click **Apply**.
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 1-7 shows the user status.

Figure 1-7 Registration status of voice users


Sequence	Line Name	Telephone Number	Associated POTS	User Status	Call Status	Interface Status
1	A0	--	1	Up	Idle	Inservice
2	A1	--	2	Up	Idle	

- Configure the ONT on the U2000.
 1. Log in to the U2000 and enable the FTP service.
 2. Add an ONT general VAS configuration profile.

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.

- a. Choose **Configuration > Access Profile Management** from the main menu. In the window that is displayed, choose **PON Profile > ONT VAS Profile** from the navigation tree.
- b. Click the **General ONT VAS Profile** tab.
- c. Right-click in the information list and choose **Add** from the shortcut menu.
- d. In the dialog box that is displayed, set the parameters.
 - Name: *HG8240*

- Choose **General Para > WAN Device > WAN Interface 1 > WAN Connection** from the navigation tree. Right-click **WAN Connection** and choose **Add IP Connection** from the shortcut menu. Select **WAN IP Connection 1** and configure the following parameters:
 - WAN Enable: *Enable*
 - Connection Type: *Routed*
 - VLAN ID: *300*
 - Priority: *5*
 - Choose **General Para > Services > Voice Service > Voice Service 1 > Interface Configuration > Interface 1** from the navigation tree and configure the following parameters:
 - Signaling Protocol: *H248*
 - Associate WAN Interface: *WAN1*
 - Choose **General Para > Services > Voice Service > Voice Service 1 > Interface Configuration > Interface 1 > H248** from the navigation tree and configure the following parameters:
 - Primary MGC: *200.200.200.200*
 - MID Format: *Domain Name*
 - Choose **General Para > Services > Voice Service > Voice Service 1 > Interface Configuration > Interface 1 > User** from the navigation tree and select the **User** node.
 - Click **User 1**. Set **User Enabled** to **Enabled** and **Interface ID** to **1**, indicating that the TEL1 port on the ONT is bound.
 - Click **User 2**. Set **User Enabled** to **Enabled** and **Interface ID** to **2**, indicating that the TEL2 port on the ONT is bound.
 - Choose **General Para > Services > Voice Service > Voice Service 1 > Physical Interface** from the navigation tree. Right-click **Physical Interface** and choose **Add Physical Interface**.
- e. Click **Next**.
- f. In the dialog box that is displayed, set **vendor ID** to **HWTC**, **Terminal Type** to **HG8240**, and **Version** to **V1R002C06-V1R002Czz**. Then click **Add**.
- g. In the dialog box that is displayed, set the parameters.
- Choose **HG8240 Config Info > Services > Voice Service > Voice Service 1 > Interface Configuration > Interface 1** from the navigation tree. Set **Region** to **China**.
 - Choose **HG8240 Config Info > WAN Device > WAN Device 1 > WAN Connection > WAN Connection 1** from the navigation tree. Set **WAN Interface Name** to **ONT-VOIP**, **NATEnabled** to **Enable**, and **Service Type** to **VOIP**.
- h. Click **Finish**.
3. Bind a general VAS profile and configure VAS services.
- a. Choose **GPON > GPON Management** from the navigation tree.
 - b. On the **GPON ONU** tab, enter the search criteria or click  to query the GPON ONU records.

- c. Right-click the ONT record with **Frame** being **0**, **Slot** being **2**, **Port** being **1**, and **ONU ID** being **0** in the list and choose **Bind General VAS Profile** from the shortcut menu.
 - d. In the dialog box that is displayed, select the VAS profile with **Profile Name** being **HG8245** and click **OK**.
 - e. Right-click the ONT record and choose **Configure Value-Added Service** from the shortcut menu.
 - f. In the dialog box that is displayed, click the **Basic Parameters** tab. Select **Voice Service** and set **MG Domain name** to **32303131B39FD641**.
 - g. Click **OK**.
4. Click **OK**. In the dialog box that is displayed, click **OK**. The configuration takes effect after the device automatically restarts.

---End

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.

Prerequisite

- The SIP interface data and PSTN 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 ONT has been added to the OLT. For details, see [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

Table 1-11 Data plan

Item	Data
ONT line profile	Profile name: fth T-CONT ID: 4 GEM port ID: 12
ONT service profile	Profile name: fth ONT 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.

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. Perform this step in the **bridging ONT (single VLAN tag)** scenario.

Table 1-12 Data plan

Scenario	VLAN Plan	VLAN Translation Policy
Bridging ONT	Single VLAN tag <ul style="list-style-type: none">● VLAN ID: 300● VLAN type: smart● VLAN attribute: common	ONT: provides the VoIP service and uses the same SVLAN.

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
```

3. Perform this step in the **bridging ONT (double VLAN tags)** scenario.

Table 1-13 Data plan

Scenario	VLAN Plan	VLAN Translation Policy
Bridging ONT	Double VLAN tags <ul style="list-style-type: none"> ● 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
outbound
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
outbound
d traffic-table name ftth_voip
    
```

4. Perform this step in the **bridging ONT+HGW (single VLAN tag)** scenario.

Table 1-14 Data plan

Scenario	VLAN Plan	VLAN Translation Policy
Bridging ONT +HG	Single VLAN tag <ul style="list-style-type: none"> ● VLAN ID: 300 ● VLAN type: smart ● VLAN attribute: common ● UVLAN ID: 45 	ONT: Upstream packets of the HGW carry the user VLAN and the ONT transparently transmits the packets. OLT: implements VLAN translation: U<->S.

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 ONT line profile.

 **NOTE**

The user VLAN is the VLAN in the packets sent from the HG 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 45
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 HG through Ethernet port 1, 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
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 45, and use traffic profile **ftth_voip**.

```
huawei (config) #service-port vlan 300 gpon 0/1/0 ont 1 gemport 12 multi-
service
  user-vlan 45 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 45 inbound traffic-table name ftth_voip outbound traffic-table
  name
  ftth_voip
```

5. Perform this step in the **bridging ONT+HGW (double VLAN tags)** scenario.

Table 1-15 Data plan

Scenario	VLAN Plan	VLAN Translation Policy
Bridging ONT +HG	Double VLAN tags <ul style="list-style-type: none"> ● SVLAN ID: 300 ● SVLAN type: smart ● SVLAN attribute: stacking ● UVLAN ID: 45 ● CVLAN ID: 3001 	ONT: Upstream packets of the HGW carry the user VLAN and the ONT transparently transmits the packets. OLT: implements VLAN translation: U<->S+C.

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 ONT line profile.

 **NOTE**

The user VLAN is the VLAN in the packets sent from the HG 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 45
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 HG through Ethernet port 1, 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
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)#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, user VLAN to 45, and CVLAN 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 45 tag-transform translate-and-add inner-vlan 3001 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 45 tag-transform translate-and-add inner-vlan 3001 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 ONT 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 with the IP address of the local maintenance Ethernet port on the ONT (default: 192.168.100.1).
- b. 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.

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 1-8 shows the parameter settings.

Figure 1-8 Parameter settings on the Web page for the voice WAN interface

		New	Delete
	Connection Name	VLAN/Priority	Protocol Type
<input type="checkbox"/>	1_VOIP_R_VID_1001	1001/0	IPv4

Basic Information			
Enable Wan Connection:	<input checked="" type="checkbox"/>		
Encapsulation Mode:	<input checked="" type="radio"/> IPoE <input type="radio"/> PPPoE		
Protocol Type:	IPv4		
Mode:	Route WAN		
Service List:	VOIP		
Enable VLAN:	<input checked="" type="checkbox"/>		
VLAN ID:	300 <small>*(1-4094)</small>		
802.1p:	5		
IP Acquisition Mode:	<input type="radio"/> Static <input checked="" type="radio"/> DHCP <input type="radio"/> PPPoE		
Vendor ID:	<input type="text"/> <small>(The vendor ID must be 0 - 63 characters in length.)</small>		
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>			

- c. Click **Apply**.
3. Configure parameters for the SIP-based voice interface.
 - a. Choose **Voice > VoIP Basic Configuration**.
 - b. In the right pane, configure the parameters as follows:
 - Set **Proxy Server Address** to **200.200.200.200**.
 - Set **Home Domain** to **huawei.com**.
 - Set **Region** to **CN-China**.
 - Set **Signaling Port** to **1_VOIP_R_VID_300**.

 **NOTE**

- **Standby Server Address** must be set if dual-homing is configured.
- If you do not set **Media Port**, 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 service flows 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**.

Figure 1-9 shows the parameter settings.

Figure 1-9 Parameter settings on the Web page for the SIP-based voice interface

Outbound Proxy Address:	<input type="text"/>	(IP or Domain)
Outbound Proxy Port:	<input type="text" value="5060"/>	(0-65535)
Standby Outbound Proxy Address:	<input type="text"/>	(IP or Domain)
Standby Outbound Proxy Port:	<input type="text" value="5060"/>	(0-65535)
Primary Proxy Address:	<input type="text" value="200.200.200.200"/>	(IP or Domain)
Primary Proxy Port:	<input type="text" value="5060"/>	(0-65535)
Standby Proxy Address:	<input type="text"/>	(IP or Domain)
Standby Proxy Port:	<input type="text" value="5060"/>	(0-65535)
Home Domain:	<input type="text" value="huawei.com"/>	(IP or Domain)
Local Port:	<input type="text" value="5060"/>	*(0-65535)
Digitmap:	<input type="text" value="x.S x.#"/>	
Digitmap Match Mode:	<input type="text" value="Min"/>	
Registration Period:	<input type="text" value="600"/>	(Unit:s)(1~65534)
Region:	<input type="text" value="CN - China"/>	
Signaling Port:	<input type="text" value="2_VOIP_R_VID_300"/>	(Select the name of the WAN that will c messages.)
Media Port:	<input type="text"/>	(Select the name of the WAN that will c media port is same with signaling port when it is empty.)
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>		

- c. Click **Apply**.
4. Configure parameters for the SIP-based voice users.
 - a. Choose **Voice > VoIP Basic Configuration**.
 - b. In the **User Basic Parameters** window, set parameters for voice user 1 as follows:
 - Select **Enable User** to enable the voice user configuration.
 - Set **Register User Name** to **77730010**.
 - Set **Associated POTS** to **1**.
 - Set **Auth User Name** to **+8675577730010@huawei.com**.
 - Set **Password** to **iadtest1**.

In the right pane, 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 **Register User Name** to **77730020**.

- Set **Associated POTS** to **2**.
- Set **Auth User Name** to **+8675577730020@huawei.com**.
- Set **Password** to **iadtest2**.

Figure 1-10 shows the parameter settings.

Figure 1-10 Parameter settings on the Web page for SIP-based voice user 2

User Basic Parameters					
On this page, you can set the basic parameters for the voice users.					
					New Delete
	Sequence	Register User Name	Auth User Name	Password	Associated POTS
<input type="checkbox"/>	1	77730010	+8675577730010@huawei.com	*****	1
<input type="checkbox"/>	2	77730020	+8675577730020@huawei.com	*****	2

Enable User:

Register User Name: (Telephone Number)

Associated POTS:

Auth User Name: (The length must be between 0-64.)

Password: (The length must be between 0-64.)

Apply Cancel

- c. Click **Apply**.
5. (Optional) Configure routes.

You need to configure routes when the IP address of the ONT and that of the voice server are in different network segments.

 - a. Choose **Route > Default Route Configuration**.
 - b. Select **Enable Default Route** and set **WAN Name** to **1_VOIP_R_VID_300**.

Figure 1-11 shows the parameter settings.

Figure 1-11 Route parameter settings

Route > Default Route Configuration

On this page, you can configure the default route.

Enable Default Route:

WAN Name:

Apply Cancel

- c. Click **Apply**.
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 1-12 shows the parameter settings.

Figure 1-12 Voice service restart


Sequence	User Name(Telephone Number)	Associated POTS	User Status	Call Status
1	77730010	1	Up	Idle
2	77730020	2	Up	Idle

- Configure the ONT on the U2000.
 1. Log in to the U2000 and enable the FTP service.
 2. Configure the value-added service (VAS) configuration profile of the ONT.

NOTE

The window for configuring ONT VAS profiles varies with ONT versions, but the parameter configuration is the same. For details, see relevant ONT manuals.

- a. Choose **Configuration > Access Profile Management** from the main menu. In the window that is displayed, choose **PON Profile > ONT VAS Profile** from the navigation tree.
- b. Click the **General ONT VAS Profile** tab.
- c. Right-click in the list and choose **Add** from the shortcut menu.
- d. In the dialog box that is displayed, set the parameters.
 - Name: *HG8240*
 - Choose **General Para > WAN Device > WAN Interface 1 > WAN Connection** from the navigation tree. Right-click **WAN Connection** and choose **Add IP Connection** from the shortcut menu. Select **WAN IP Connection 1** and configure the following parameters:
 - WAN Enable: *Enable*
 - Connection Type: *Routed*
 - VLAN ID: *300*
 - Priority: *5*
 - Choose **General Para > Services > Voice Service > Voice Service 1 > Interface Configuration > Interface 1** from the navigation tree and configure the following parameters:
 - Signaling Protocol: *SIP*
 - Associate WAN Interface: *WANI*

- Choose **General Para > Services > Voice Service > Voice Service 1 > Interface Configuration > Interface 1 > SIP** from the navigation tree and configure the following parameters:
 - Proxy Server: *200.200.200.200*
 - Proxy Server Port: *5060*
 - Home Domain: *huawei.com*
 - Choose **General Para > Services > Voice Service > Voice Service 1 > Interface Configuration > Interface 1 > User** from the navigation tree and select the **User** node.
 - Click **User 1**. Set **User Enabled** to **Enabled** and **Interface ID** to **1**, indicating that the TEL1 port on the ONT is bound.
 - Click **User 2**. Set **User Enabled** to **Enabled** and **Interface ID** to **2**, indicating that the TEL2 port on the ONT is bound.
 - Choose **General Para > Services > Voice Service > Voice Service 1 > Physical Interface** from the navigation tree. Right-click **Physical Interface** and choose **Add Physical Interface** from the shortcut menu.
 - Click **Next**.
 - In the dialog box that is displayed, set **vendor ID** to **HWTC**, **Terminal Type** to **HG8240**, and **Version** to **V1R002C06-V1R002Czz**. Then click **Add**.
 - In the dialog box that is displayed, set the parameters.
 - Choose **HG8240 Config Info > Services > Voice Service > Voice Service 1 > Interface Configuration > Interface 1** from the navigation tree. Set **Region** to **China**.
 - Choose **HG8240 Config Info > WAN Device > WAN Device 1 > WAN Connection > WAN Connection 1** from the navigation tree. Set **WAN Interface Name** to **ONT-VOIP**, **NATEnabled** to **Enable**, and **Service Type** to **VOIP**.
3. Bind the VAS profile and configure value-added services.
- a. Choose **GPON > GPON Management** from the navigation tree.
 - b. On the **GPON ONU** tab, enter the search criteria or click  to query the GPON ONU records.
 - c. Right-click an ONT record in the list and choose **Bind General VAS Profile** from the shortcut menu.
 - d. In the dialog box that is displayed, select the VAS profile with **Profile Name** being **HG8240** and click **OK**.
 - e. Right-click the ONT record and choose **Configure Value-Added Service** from the shortcut menu.
 - f. In the dialog box that is displayed, set the parameters.

On the **Basic Parameters** tab, select **Voice Service**.

 - Set **Auth User Name** to **+8675577730010@huawei.com**, **Directory Number** to **77730010**, and **Password** to **iadtest1** for **Interface ID 1**.
 - Set **Auth User Name** to **+8675577730020@huawei.com**, **Directory Number** to **77730020**, and **Password** to **iadtest2** for **Interface ID 2**.

g. Click **OK**.

----End

Configuring the SIP-based VoIP Service (Through the CLI)

The OLT uses the OMCI protocol to manage ONTs and apply VoIP configurations to ONTs.

Data Plan

Table 1-16 Data plan

Item	Data
ONT line profile	Profile name: fthh T-CONT ID: 4 GEM port ID: 12
ONT service profile	Profile name: fthh ONT port capability set: adaptive
Voice parameter	IP address of the SIP server: 200.200.200.200/24 Port ID of the SIP server: 5060 User phone number 1: 88881111 User phone number 2: 88882222

Prerequisite

- The data for interconnecting with the SIP interface is 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 [Adding an ONT to an OLT](#).
- The ONT software version must support the configuration. Currently, only the V100R002C02 version supports the configuration.

Procedure

Step 1 Configure a VLAN translation policy and service flows.

1. Perform this step in the **bridging ONT (single VLAN tag)** scenario.

Table 1-17 Data plan

Scenario	VLAN Plan	VLAN Translation Policy
Bridging ONT	Single VLAN tag <ul style="list-style-type: none">● VLAN ID: 300● VLAN type: smart● VLAN attribute: common	ONT: provides the VoIP service and uses the same SVLAN.

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 1-18 Data plan

Scenario	VLAN Plan	VLAN Translation Policy
Bridging ONT	Double VLAN tags <ul style="list-style-type: none">● 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
outbound
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
outbound
d traffic-table name ftth_voip

```

3. Perform this step in the **bridging ONT+HGW (single VLAN tag)** scenario.

Table 1-19 Data plan

Scenario	VLAN Plan	VLAN Translation Policy
Bridging ONT+HG	Single VLAN tag <ul style="list-style-type: none"> ● VLAN ID: 300 ● VLAN type: smart ● VLAN attribute: common ● UVLAN ID: 45 	ONT: Upstream packets of the HGW carry the user VLAN and the ONT transparently transmits the packets. OLT: implements VLAN translation: U<->S.

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 ONT line profile.

 **NOTE**

The user VLAN is the VLAN in the packets sent from the HG 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 45
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 HG through Ethernet port 1, 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
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 45, and use traffic profile **ftth_voip**.

```

huawei(config)#service-port vlan 300 gpon 0/1/0 ont 1 gemport 12 multi-service
user-vlan 45 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 45 inbound traffic-table name ftth_voip outbound traffic-table name
ftth_voip

```

4. Perform this step in the **bridging ONT+HGW (double VLAN tags)** scenario.

Table 1-20 Data plan

Scenario	VLAN Plan	VLAN Translation Policy
Bridging ONT+HG	Double VLAN tags <ul style="list-style-type: none"> ● SVLAN ID: 300 ● SVLAN type: smart ● SVLAN attribute: stacking ● UVLAN ID: 45 ● CVLAN ID: 3001 	ONT: Upstream packets of the HGW carry the user VLAN and the ONT transparently transmits the packets. OLT: implements VLAN translation: U<->S+C.

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 ONT line profile.

 **NOTE**

The user VLAN is the VLAN in the packets sent from the HG to the ONT, that is, the UVLAN.

```
huawei(config)#ont-lineprofile gpon profile-name fthh
huawei(config-gpon-lineprofile-1)#gem mapping 12 2 vlan 45
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 HG through Ethernet port 1, add Ethernet port 1 to VLAN 45 in the ONT service profile.

```
huawei(config)#ont-srvprofile gpon profile-name fthh
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)#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, user VLAN to 45, and CVLAN to 3001. Use traffic profile **fthh_voip**.

```
huawei(config)#service-port vlan 300 gpon 0/1/0 ont 1 gempport 12 multi-
service
user-vlan 45 tag-transform translate-and-add inner-vlan 3001 inbound traffic-
table
name fthh_voip outbound traffic-table name fthh_voip
huawei(config)#service-port vlan 300 gpon 0/1/0 ont 2 gempport 12 multi-
service
user-vlan 45 tag-transform translate-and-add inner-vlan 3001 inbound traffic-
table
name fthh_voip outbound traffic-table name fthh_voip
```

Step 2 (Optional) Configure global media attributes.

Set the fax mode to transparent transmission and the maximum jitter buffer to 200 ms. Use default values for other parameters.

```
huawei(config)#ont-voip-media attribute faxmode passthru jitter-buffer max 200
```

Step 3 Configure the IP addresses of ONT SIP users.

```
huawei(config)#interface gpon 0/1
huawei(config-if-gpon-0/1)#ont ipconfig 0 1 static ip-address 10.10.10.10 mask
```

```
255.255.255.0 vlan 20
huawei(config-if-gpon-0/1)#ont ipconfig 0 2 static ip-address 10.10.10.20 mask
255.255.255.0 vlan 20
huawei(config-if-gpon-0/1)#quit
```

Step 4 Configure ONT voice service profiles.

The ONT voice service profiles include the digitmap profile, SIP agent profile, and POTS profile.

- The digitmap profile contains the digitmap information of the ONT, including the digitmap format and timeout time of the digitmap timer.
- The SIP agent profile contains the SIP agent information of the ONT, including the SIP agent server, signaling transmission mode, and signaling transmission port.
- The POTS profile contains the physical attributes of POTS ports on the ONT, including the port impedance and port signaling type.

1. Configure a digitmap profile.

Run the **display ont-digitmap-profile** command to query the existing digitmap profiles in the system. If the existing digitmap profiles in the system do not meet the requirements, run the **ont-digitmap-profile add** command to add a digitmap profile.

Create digitmap profile 2 with the internal digitmap format of the ONT.

```
huawei(config)#ont-digitmap-profile add profile-id 2 digitmap-format
not_defined
```

2. Configure a SIP agent profile.

Run the **display ont-sipagent-profile** command to query the existing SIP agent profiles in the system. If the existing SIP agent profiles do not meet the requirements, run the **ont-sipagent-profile add** command to add a SIP agent profile.

Create SIP agent profile 2, set the IP address of the SIP server to 200.200.200.200 and signaling port ID to 5060, and use default values for other parameters.

```
huawei(config)#ont-sipagent-profile add profile-id 2 proxy-server
200.200.200.200 signal signal-port 5060
```

3. Configure a POTS profile.

Run the **display ont-pots-profile** command to query the existing POTS profiles in the system. If the existing POTS profiles in the system do not meet the requirements, run the **ont-pots-profile add** command to add a POTS profile.

In this example, the default POTS profile, namely POTS profile 1 is used.

Step 5 Configure SIP PSTN users.

1. Add PSTN users.

Add PSTN user **huawei1** (phone number: 88881111) and PSTN user **huawei2** (phone number: 88882222) on ONT1 and ONT2 respectively.

```
huawei(config)#interface gpon 0/1
huawei(config-if-gpon-0/1)#sippstnuser add 0 1 1 username huawei1 telno
88881111
huawei(config-if-gpon-0/1)#sippstnuser add 0 2 1 username huawei2 telno
88882222
```

2. Bind ONT voice service profiles to PSTN users.

The ONT voice service profiles include the digitmap profile, SIP agent profile, and POTS profile. By default, a new PSTN user is bound to SIP agent profile 1, digitmap profile 1, and POTS profile 1. If the default profiles do not meet the requirements, bind other profiles. Bind digitmap profile 2 and SIP agent profile 2 to the PSTN user. Use the default POTS profile.

```
huawei(config-if-gpon-0/1)#sippstnuser digitmap 1 1 1 digitmap-profile profile-
id 2
huawei(config-if-gpon-0/1)#sippstnuser digitmap 0 2 1 digitmap-profile profile-
```

```
id 2
huawei(config-if-gpon-0/1)#sippstnuser ipconfig 0 1 1 sip-agent-profile
profile-id 2
huawei(config-if-gpon-0/1)#sippstnuser ipconfig 0 2 1 sip-agent-profile
profile-id 2
huawei(config-if-gpon-0/1)#quit
```

Step 6 Save the data.

```
huawei(config)#save
```

---End

Configuring the BTV Multicast Service

The OLT is connected to the remote bridging ONT through a GPON port to provide users with the multicast service.

Prerequisites

- The license for the multicast program or the multicast user has already been requested and installed.
- 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 [Adding an ONT to an OLT](#).

Data Plan

Table 1-21 Data plan

Item	Data
ONT line profile	Profile name: fth T-CONT ID: 4 GEM port ID: 13
ONT service profile	Profile name: fth ONT 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

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. Perform this step in the **bridging+voice ONT (single VLAN tag)** scenario.

Table 1-22 Data plan

VLAN Plan	VLAN Translation Policy
<ul style="list-style-type: none"> ● SVLAN ID: 1000 ● VLAN type: smart ● VLAN attribute: common 	<p>ONT: duplicates packets based on user ports and multicast VLANs (MVLANS) are stripped off downstream.</p> <p>OLT: duplicates multicast packets based on PON ports with MVLAN unchanged.</p>

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)#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
```

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 gempport 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 gempport 13 multi-
```

```
service
  user-vlan untagged rx-cttr 8 tx-cttr 8
```

3. Perform this step in the **bridging ONT+HG (single VLAN tag)** scenario.

Table 1-23 Data plan for the scenario in which the HG MVLAN differs from the network-side MVLAN

VLAN Plan	VLAN Translation Policy
<ul style="list-style-type: none"> ● SVLAN ID: 1000 ● HG VLAN: 43 ● VLAN type: smart ● VLAN attribute: common 	<p>ONT: translates the upstream VLAN of the HG to an MVLAN.</p> <p>OLT: duplicates multicast packets based on PON ports with MVLAN unchanged.</p>

Configure the mapping relationship between a GEM port and a VLAN. If the ONT is connected to the HG 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
```

Configure a VLAN translation policy for the Ethernet port on the ONT. If the ONT is connected to the HG through Ethernet port 2, VLAN 43 of the HG 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
```

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 gempport 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 gempport 13 multi-
service
  user-vlan 1000 rx-cttr 8 tx-cttr 8
```


Table 1-24 Data plan for the scenario in which the HG MVLAN is the same as the network-side MVLAN

VLAN Plan	VLAN Translation Policy
<ul style="list-style-type: none"> ● SVLAN ID: 1000 ● VLAN type: smart ● VLAN attribute: common 	<p>ONT: transparently transmits the MVLAN of the HG. Multicast packets are duplicated downstream with MVLAN unchanged.</p> <p>OLT: duplicates multicast packets based on PON ports with MVLAN unchanged.</p>

Configure the mapping relationship between a GEM port and a VLAN. If the ONT is connected to the HG 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
```

Configure a VLAN translation policy for the Ethernet port on the ONT. If the ONT is connected to the HG through Ethernet port 2, the multicast forwarding mode is VLAN tag.

```
huawei(config)#ont-srvprofile gpon profile-name ftth
huawei(config-gpon-srvprofile-1)#multicast-forward tag
huawei(config-gpon-srvprofile-1)#port vlan eth 2 vlan 1000
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 gempport 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 gempport 13 multi-
service
user-vlan 1000 rx-cttr 8 tx-cttr 8
```

4. 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
```

5. 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
```

6. 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
```

7. 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
```

8. (Optional) Set multicast global parameters.

In this example, the default settings are used for all the multicast global parameters.

9. 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
```

10. Save the data.

```
huawei(config)#save
```

- The ONT does not need to be configured.

----End

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 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 [Adding an ONT to an OLT](#).

Data Plan

Table 1-25 Data plan

Item	Data
ONT line profile	Profile name: fthh T-CONT ID: 4 GEM port ID: 13
ONT service profile	Profile name: fthh ONT 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 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. Perform this step in the **bridging+voice ONT (single VLAN tag)** scenario.

Table 1-26 Data plan

VLAN Plan	VLAN Translation Policy
<ul style="list-style-type: none"> ● SVLAN ID: 1100 ● VLAN type: smart ● VLAN attribute: common ● CVLAN=SVLAN 	<p>ONT: adds CVLAN tags to iTV service packets.</p> <p>OLT: transparently transmits packets with SVLANs.</p>

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 fttth
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 fttth
huawei(config-gpon-srvprofile-1)#port vlan eth 2 1100
huawei(config-gpon-srvprofile-1)#multicast-forward tag
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
```

3. Perform this step in the **bridging+voice ONT (double VLAN tags)** scenario.

Table 1-27 Data plan

VLAN Plan	VLAN Translation Policy
<ul style="list-style-type: none"> ● SVLAN ID: 1100 ● VLAN type: smart ● VLAN attribute: stacking ● C'VLAN: 2010 ● CVLAN: 2001 	<p>ONT: adds the same CVLAN tag to packets.</p> <p>OLT: implements VLAN translation: C<->S+C'.</p>

Configure the mapping relationship between a GEM port and a VLAN. The service flow of user VLAN 2001 is mapped to GEM port 13 in the ONT line profile.

```
huawei(config)#ont-lineprofile gpon profile-name fttth
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 ONT. If the ONT is connected to the STB through Ethernet port 2, add Ethernet port 2 to VLAN 2001.

```

huawei(config)#ont-srvprofile gpon profile-name ftth
huawei(config-gpon-srvprofile-1)#port vlan eth 2 2001
huawei(config-gpon-srvprofile-1)#multicast-forward tag translation 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

```

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 2001.

```

huawei(config-if-gpon-0/1)#ont port native-vlan 1 1 eth 2 vlan 2001
huawei(config-if-gpon-0/1)#ont port native-vlan 1 2 eth 2 vlan 2001
huawei(config-if-gpon-0/1)#quit

```

Create service flows. Set the service VLAN to 1100, GEM port ID to 13, and user VLAN to 1100, and use traffic profile 8.

```

huawei(config)#service-port 3 vlan 1100 gpon 0/1/0 ont 1 gemport 13 multi-
service
user-vlan 2001 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 rx-cttr 8 tx-cttr 8

```

Configure a VLAN translation policy for the service flow. Set the VLAN translation policy to Translate and Add. The CVLAN 2001 of the ONT is translated to C'VLAN 2010.

```

huawei(config)#service-port 3 tag-transform translate-and-add inner-vlan 2010
huawei(config)#service-port 4 tag-transform translate-and-add inner-vlan 2010

```

4. Perform this step in the **bridging ONT+HG (single VLAN tag)** scenario.

Table 1-28 Data plan

VLAN Plan	VLAN Translation Policy
<ul style="list-style-type: none"> ● SVLAN ID: 1100 ● VLAN type: smart ● VLAN attribute: common ● UVLAN (upstream VLAN of the HG): 43 ● CVLAN=UVLAN 	<p>ONT: transparently transmits the UVLAN of the HG.</p> <p>OLT: implements VLAN translation: U<->S.</p>

Configure the mapping relationship between a GEM port and a VLAN. The service flow of user VLAN 43 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 43
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 HG through Ethernet port 2, add Ethernet port 2 to VLAN 43.

```

huawei(config)#ont-srvprofile gpon profile-name ftth
huawei(config-gpon-srvprofile-1)#port vlan eth 2 43

```

```
huawei (config-gpon-srvprofile-1)#multicast-forward tag translation 43
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 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 multi-
service
user-vlan 43 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 43 rx-cttr 8 tx-cttr 8
```

5. Perform this step in the **bridging ONT+HG (double VLAN tags)** scenario.

Table 1-29 Data plan

VLAN Plan	VLAN Translation Policy
<ul style="list-style-type: none"> ● SVLAN ID: 1100 ● VLAN type: smart ● VLAN attribute: common ● UVLAN (upstream VLAN of the HG): 43 ● CVLAN: 2010 	<p>ONT: transparently transmits the UVLAN of the HG.</p> <p>OLT: implements VLAN translation: U<->S+C.</p>

Configure the mapping relationship between a GEM port and a VLAN. The service flow of user VLAN 43 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 43
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 HG through Ethernet port 2, add Ethernet port 2 to VLAN 43.

```
huawei (config)#ont-srvprofile gpon profile-name ftth
huawei (config-gpon-srvprofile-1)#port vlan eth 2 43
huawei (config-gpon-srvprofile-1)#multicast-forward tag translation 43
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 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 multi-
service
```

```
user-vlan 43 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 43 rx-cttr 8 tx-cttr 8
```

Configure a VLAN translation policy for the service flow. Set the VLAN translation policy to Translate and Add to translate the UVLAN 43 of the HG to CVLAN 2010.

```
huawei(config)#service-port 3 tag-transform translate-and-add inner-vlan 2010
huawei(config)#service-port 4 tag-transform translate-and-add inner-vlan 2010
```

6. Save the data.

```
huawei(config)#save
```

Step 2 The ONT does not need to be configured.

---End

Configuring Link Aggregation, Congestion Control, and Security Policy

Service reliability is improved by configuring uplink aggregation and priority scheduling policy for upstream queues in global configuration mode, and service security is improved by configuring security policy in global configuration mode.

Background Information

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 [2.2.1 Security Design](#).

Procedure

- Configure link aggregation.
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.
According to "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 anti-DoS-attack.
 1. Run the **security anti-dos enable** command to enable global anti-DoS attack.
 2. Run the **security anti-dos control-packet policy** command to configure the policy of processing protocol packets when a DoS attack occurs.

3. Run the **security anti-dos control-packet rate** command to configure the threshold of the rate for sending protocol packets to the CPU.
- Enable anti-ICMP-attack.
Run the **security anti-icmpattack enable** command to enable anti-ICMP attack.
 - Enable anti-IP-attack.
Run the **security anti-ipattack enable** command to enable anti-IP attack.
- Configure user security.
 - Enable anti-MAC-duplicate.
Run the **security anti-macduplicate enable** command to enable anti-MAC-duplicate.
 - Enable anti-IP spoofing.
The anti-IP spoofing function can be enabled or disabled at three levels. This anti-IP spoofing function takes effect only when it is enabled at all three levels.
 1. Global level: Run the **security anti-ipspoofing enable** command in global configuration mode.
 2. VLAN level: Run the **security anti-ipspoofing enable** command in VLAN service profile configuration mode.
 3. Service port level: Run the **security anti-ipspoofing service-port serviceport-id enable** command.
 - Configure service security.
 - Enable DHCP Option82.
The DHCP option 82 function can be enabled or disabled at four levels. The DHCP option 82 function takes effect only when it is enabled at all four levels.
 1. Global level: Run the **dhcp option82 enable** command in global configuration mode.
 2. Port level: Run the **dhcp option82 port** or **dhcp option82 board** command to enable the function at the port level.
 3. VLAN level: Run the **dhcp option82 enable** command in VLAN service profile configuration mode.
 4. Service port level: Run the **dhcp option82 service-port** command.
 - Enable PITP.
The PITP function can be enabled or disabled at four levels. The PITP function takes effect only when it is enabled at all four levels.
 1. Global level: Run the **pitp enable pmode** command in global configuration mode.
 2. Port level: Run the **pitp port** or **pitp board** command to enable the function at the port level.
 3. VLAN level: Run the **pitp enable** command in VLAN service profile configuration mode.
 4. Service port level: Run the **pitp service-port** command.

----End

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.	<ul style="list-style-type: none"> ● 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.	<ul style="list-style-type: none"> ● An ONT can simulate the caller or callee in a call to a phone. Only a functioning phone is required in the central equipment room. ● 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 emulation 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>|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    : -
Emulator 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 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.
 - b. 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.
 - c. 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.
- 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 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 : 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 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.

- a. Run the **display mac-address vlan** command to check the MAC address learning status of the voice service VLAN.
 - b. 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.
 - c. If the downstream port does not learn a MAC address, check whether the ONT is activated and whether physical links are normal.
 - d. 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.
 - e. If an IP address is allocated to the MAC address and there is a session border controller (SBC) on the network, log in to the SBC to check whether the voice service of the ONT is registered.
 - f. If the registration status is registering, check the voice configurations on the MGC/SIP server are consistent with those on the ONT. If there is no registration information, log in to the ONT onsite or remotely and check whether VoIP configurations are applied to 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  
Command is being executed. Please wait...  
Multicast flow statistic result: 8736(kbps)
```

---End

1.2.3 Gateway ONT Network Scenario

This topic describes how to configure Internet access services, voice services, and video services when gateway ONTs are used to build an FTTH network.

Service Requirements and Application Scenario

When a gateway ONT is used to build an FTTH network, the ONT functions as a home gateway unit (HGU) in the upstream direction of PON ports. An integrated access device (IAD) is built in the ONT, providing high-speed Internet access services, VoIP services, and IPTV services.

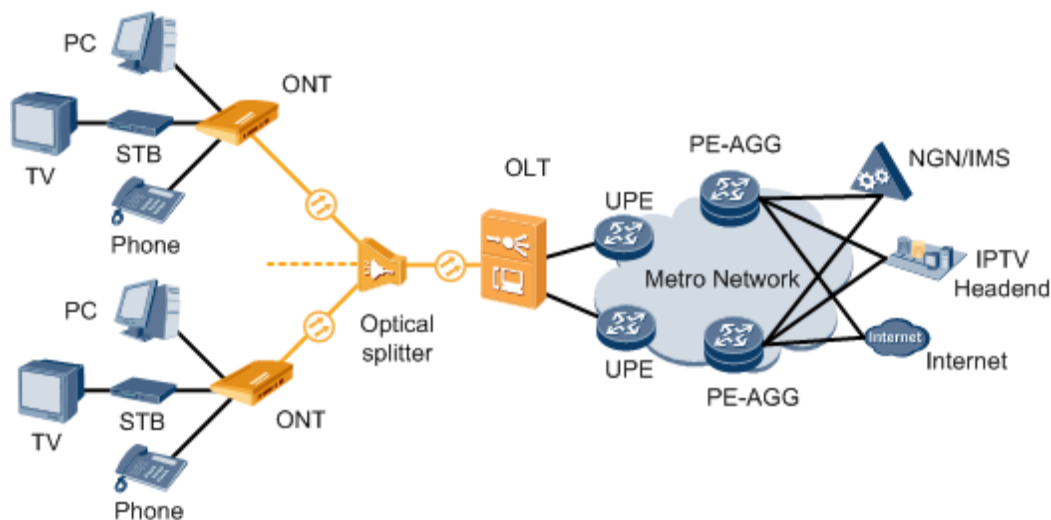
Service Requirements

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

Figure 1-13 Home gateway



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 1-30 Data plan

Item	Data
DBA profile	Profile name: fthfth_dba Profile type: type3 Assured bandwidth: 8 Mbit/s Maximum bandwidth: 20 Mbit/s
ONT line profile	Profile name: fthh 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: fthh 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.

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

- 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.
- 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.
- 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  
-----  
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.

 **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.

----End

Configuring the Layer 3 Internet Access Service

The OLT is connected to the remote ONT 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 configurations, see the configuration guide.
- The ONT has been added to the OLT. For details, see [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.

Context

Table 1-31 Data Plan

Item	Data
ONT line profile	Profile name: fthh T-CONT ID: 4 GEM port ID: 14
ONT service profile	Profile name: fthh ONT 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 fthh_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 fthh_hsi cir 4096 priority 0 priority-policy local-setting
```

2. Perform this step in the **gateway ONT (double VLAN tags)** scenario.

Table 1-32 Scenario plan

Scenario	VLAN Plan	VLAN Translation Policy
Scenario 1	Double VLAN tags <ul style="list-style-type: none"> ● 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 <ul style="list-style-type: none"> ● 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 gempport 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 gempport 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 fttth
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 native VLAN of the ONT port. If the ONT is connected to a PC through Ethernet port 1, the native VLAN ID is 1001.

```
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
```

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 fttth_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 fttth_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 fttth_hsi
```

3. Save the data.

```
huawei(config)#save
```

● Configure the ONT on the Web page.

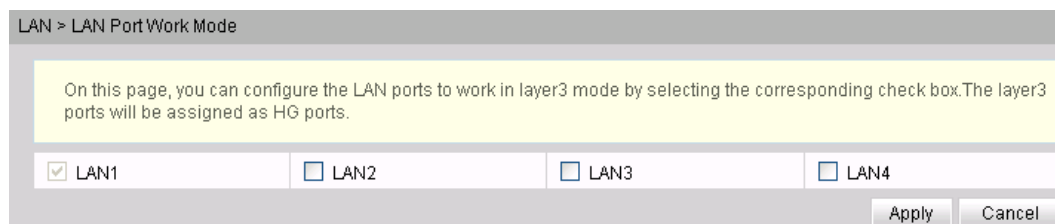
1. Log in to the Web configuration window.

- a. Configure the IP address of the PC network adapter to be in the same network segment with the IP address of the local maintenance Ethernet port on the ONT (default: 192.168.100.1).
- b. 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.

2. Configure the working mode for a LAN port.

- a. 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 1-14** shows the parameter settings.

Figure 1-14 Parameter settings on the Web page for the LAN port



- b. Click **Apply** to make the configuration take effect.
3. Configure parameters for a WAN interface.
 - a. Choose **WAN > WAN Configuration** from the navigation tree.
 - 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 **PPPOE**.
 - 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.
 - Set **IP Acquisition Mode** to **PPPoE**.
 - Select **Enable NAT** to enable the NAT function.

Figure 1-15 shows the parameter settings.

Figure 1-15 Parameter settings on the Web page for the WAN port

		New	Delete
Connection Name	VLAN/Priority	Protocol Type	
Basic Information			
Enable Wan Connection:	<input checked="" type="checkbox"/>		
Encapsulation Mode:	<input type="radio"/> IPoE <input checked="" type="radio"/> PPPoE		
Protocol Type:	IPv4		
Mode:	Route WAN		
Service List:	INTERNET		
Enable VLAN:	<input checked="" type="checkbox"/>		
VLAN ID:	1001 <small>*(1-4094)</small>		
802.1p:	0		
User Name:	iadtest@pppoe		
Password:	••••••		
Binding options:	<input checked="" type="checkbox"/> LAN1 <input type="checkbox"/> LAN2 <input type="checkbox"/> LAN3 <input type="checkbox"/> LAN4		
IP Acquisition Mode:	<input type="radio"/> Static <input type="radio"/> DHCP <input checked="" type="radio"/> PPPoE		
Enable NAT:	<input checked="" type="checkbox"/>		
Dial Method:	Auto		
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>			

- c. Click **Apply** to make the configuration take effect.

4. Check the connection status.

Choose **Status > WAN Information** from the navigation tree. In the right pane, **Connected** is displayed in the **Status** row and the obtained IP address is displayed in the **IP Address** row.

Figure 1-16 shows the connection status of the Layer 3 Internet access service.

Figure 1-16 Connection status of Layer 3 Internet access service

Status > WAN Information							
On this page, you can query the connection status and line status of the WAN interface.							
IPv4 Information							
WAN Name	Status	IP Acquisition Mode	IP Address	Subnet Mask	VLAN/Priority	MAC Address	Connect
1_INTERNET_R_VID_1001	Connected	PPPoE	172.16.100.178	255.255.255.0	1001/0	78:1D:BA:55:64:F7	AlwaysOn

----End

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.

Prerequisite

- The port data and the PSTN user data corresponding to the MG port have been configured on the MGC.
- The OLT must be 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 [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

Table 1-33 Data Plan

Item	Data
ONT line profile	Profile name: fthh T-CONT ID: 4 GEM port ID: 12
ONT service profile	Profile name: fthh ONT port capability set: adaptive

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. Perform this step in the **gateway ONT (single VLAN tag)** scenario.

Table 1-34 Scenario plan

Scenario	VLAN Plan	VLAN Translation Policy
Scenario 1	Single VLAN tag <ul style="list-style-type: none"> ● 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 <ul style="list-style-type: none"> ● 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
```

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
```

3. 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
```

4. Save the data.

```
huawei(config)#save
```

● Configure the ONT 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 with the IP address of the local maintenance Ethernet port on the ONT (default: 192.168.100.1).
- b. 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.

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 1-17 shows the parameter settings.

Figure 1-17 Parameter settings on the Web page for the voice WAN interface

		New	Delete
	Connection Name	VLAN/Priority	Protocol Type
<input type="checkbox"/>	1_VOIP_R_VID_1001	1001/0	IPv4
Basic Information			
Enable Wan Connection:	<input checked="" type="checkbox"/>		
Encapsulation Mode:	<input checked="" type="radio"/> IPoE <input type="radio"/> PPPoE		
Protocol Type:	IPv4		
Mode:	Route WAN		
Service List:	VOIP		
Enable VLAN:	<input checked="" type="checkbox"/>		
VLAN ID:	300 <small>*(1-4094)</small>		
802.1p:	5		
IP Acquisition Mode:	<input type="radio"/> Static <input checked="" type="radio"/> DHCP <input type="radio"/> PPPoE		
Vendor ID:	<input type="text"/> <small>(The vendor ID must be 0 - 63 characters in length.)</small>		
		Apply	Cancel

- c. Click **Apply**.
3. Configure parameters for the H.248-based voice interface.
 - a. Choose **Voice > VoIP Basic Configuration**.
 - b. In the right pane, configure the parameters as follows:
 - Set **Primary MGC Address** to **200.200.200.200**.
 - Set **MID Format** to **DomainName** and **MG Domain** to **huawei.com**.
 - Set **Signaling Port** to **1_VOIP_R_VID_300**.
 - Set **Region** to **CN-China**.

Figure 1-18 shows the parameter settings.

Figure 1-18 Parameter settings on the Web page for the H.248-based voice interface

Interface Basic Parameters	
On this page, you can set the basic parameters for the voice interface.	
Primary MGC Address:	200.200.200.200 *(IP or Domain)
Primary MGC Port:	2944 *(0-65535)
Standby MGC Address:	(IP or Domain)
Standby MGC Port:	2944 (0-65535)
MG Domain:	huawei.com
Local Port:	2944 *(0-65535)
Device Name:	
MID Format:	DomainName
Digitmap Match Mode:	Min
Digitmap Auto Match Enable:	<input type="checkbox"/>
RTP TID Prefix:	0
Start Number of RTP TID:	0
Width of RTP TID Number:	6
Signaling Port:	2_VOIP_R_VID_300 (Select the name of the WAN that v messages.)
Media Port:	(Select the name of the WAN that v media port name is same with signaling port name when it is
Region:	CN - China
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

- c. Click **Apply**.
4. Configure parameters for H.248-based voice users.
 - a. Choose **Voice > VoIP Basic Configuration**.
 - b. In the right pane, click **New**. In the dialog box that is displayed, set the parameters for user 1 as follows:
 - Select **Enable Line Name**.
 - Set **Line Name** to **A0**.
 - Set **Associated POTS** to **1**.
 - Click **Apply**.

In the right pane, click **New** to add voice user 2, and set the parameters for voice user 2 as follows:

- Select **Enable Line Name**.

- Set **Line Name** to **A1**.
- Set **Associated POTS** to **2**.
- Click **Apply**.

Figure 1-19 shows the parameter settings.

Figure 1-19 Parameter settings on the Web page for H.248-based voice users

User Basic Parameters

On this page, you can set the basic parameters for the voice users.

	Sequence	Line Name	Associated POTS
<input type="checkbox"/>	1	A0	1
<input type="checkbox"/>	2	A1	2

Enable Line Name:

Line Name: *

Associated POTS:

- c. Click **Apply**.
5. (Optional) Configure routes.

You need to configure routes when the IP address of the ONT and that of the voice server are in different network segments.

 - a. Choose **Route > Default Route Configuration**.
 - b. Select **Enable Default Route** and set **WAN Name** to **1_VOIP_R_VID_300**.

Figure 1-20 shows the parameter settings.

Figure 1-20 Route parameter settings

Route > Default Route Configuration

On this page, you can configure the default route.

Enable Default Route:

WAN Name:

- c. Click **Apply**.
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 1-21 shows the user status.

Figure 1-21 Registration status of voice users


Sequence	Line Name	Telephone Number	Associated POTS	User Status	Call Status	Interface Status
1	A0	--	1	Up	Idle	Inservice
2	A1	--	2	Up	Idle	

- Configure the ONT on the U2000.
 1. Log in to the U2000 and enable the FTP service.
 2. Configure the value-added service (VAS) configuration profile of the ONT.

 **NOTE**

The window for configuring ONT VAS profiles varies with ONT versions, but the parameter configuration is the same. For details, see relevant ONT manuals.

- a. Choose **Configuration > Access Profile Management** from the main menu. In the navigation tree on the left in the window that is displayed, choose **PON Profile > ONT VAS Profile**.
- b. Click the **General ONT VAS Profile** tab.
- c. Right-click in the list and choose **Add** from the shortcut menu.
- d. In the dialog box that is displayed, set the parameters.
 - Profile name: *HG8245*
 - Choose **General Para > WAN Device > WAN Interface 1 > WAN Connection** from the navigation tree. Right-click **WAN Connection** and choose **Add IP Connection** from the shortcut menu. Select **WAN IP Connection 1** and configure the following parameters:
 - WAN Enable: *Enable*
 - Connection Type: *Routed*
 - Vlan ID: *300*
 - Priority: *5*
 - Choose **General Para > Services > Voice Service > Voice Service 1 > Interface Configuration > Interface 1** from the navigation tree and configure the following parameters:
 - Signaling Protocol: *H248*
 - Associate WAN Interface: *WANI*
 - Choose **General Para > Services > Voice Service > Voice Service 1 > Interface Configuration > Interface 1 > H248** from the navigation tree and configure the following parameters:
 - Primary MGC: *200.200.200.200*

- MID Format: *Domain Name*
 - Choose **General Para > Services > Voice Service > Voice Service 1 > Interface Configuration > Interface 1 > User** from the navigation tree and select the **User** node.
 - Click **User 1**. Set **User Enabled** to **Enabled** and **Interface ID** to **1**, indicating that the TEL1 port on the ONT is bound.
 - Click **User 2**. Set **User Enabled** to **Enabled** and **Interface ID** to **2**, indicating that the TEL2 port on the ONT is bound.
 - Choose **General Para > Services > Voice Service > Voice Service 1 > Physical Interface** from the navigation tree. Right-click **Physical Interface** and choose **Add Physical Interface** from the shortcut menu.
- e. Click **Next**.
- f. In the dialog box that is displayed, set **vendor ID** to **HWTC**, **Terminal Type** to **HG8245**, and **Version** to **V1R002C06-V1R002Czz**. Then click **Add**.
- g. In the dialog box that is displayed, set the parameters.
 - Choose **HG8245 Config Info > Services > Voice Service > Voice Service 1 > Interface Configuration > Interface 1** from the navigation tree. Set **Region** to **China**.
 - Choose **HG8245 Config Info > WAN Device > WAN Device 1 > WAN Connection > WAN Connection 1** from the navigation tree. Set **WAN Interface Name** to **ONT-VOIP**, **NATEnabled** to **Enable**, and **Service Type** to **VOIP**.
- h. Click **Finish**.
3. Bind the general VAS profile and configure value-added service.
 - a. Choose **GPON > GPON Management** from the navigation tree.
 - b. On the **GPON ONU** tab, enter the search criteria or click  to query the GPON ONU records.
 - c. Right-click the ONT record with **Frame** being **0**, **Slot** being **2**, **Port** being **1**, and **ONU ID** being **0** in the list and choose **Bind General VAS Profile** from the shortcut menu.
 - d. In the dialog box that is displayed, select the VAS profile with **Profile Name** being **HG8245** and click **OK**.
 - e. Right-click the ONT record and choose **Configure Value-Added Service** from the shortcut menu.
 - f. In the dialog box that is displayed, click the **Basic Parameters** tab. Select **Voice Service** and set **MG Domain name** to **32303131B39FD641**.
 - g. Click **OK**.
4. Click **OK**. In the dialog box that is displayed, click **OK**. The configuration takes effect after the device automatically restarts.

----End

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.

Prerequisite

- The SIP port data and the PSTN user data corresponding to the MG port have been configured on the SIP server.
- The connection between the OLT and the SIP server has been 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 [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

Table 1-35 Data plan

Item	Data
ONT line profile	Profile name: ftth T-CONT ID: 4 GEM port ID: 12
ONT service profile	Profile name: ftth ONT 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.

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. Perform this step in the **gateway ONT (single VLAN tag)** scenario.

Table 1-36 Scenario plan

Scenario	VLAN Plan	VLAN Translation Policy
Scenario 1	Single VLAN tag <ul style="list-style-type: none"> ● 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 <ul style="list-style-type: none"> ● 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

```

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 gempport 12 multi-
service
user-vlan 3001 tag-transform translate inbound traffic-table name
ftth_voip outbound
d traffic-table name ftth_voip
huawei(config)#service-port vlan 300 gpon 0/1/0 ont 2 gempport 12 multi-
service
user-vlan 3001 tag-transform translate inbound traffic-table name
ftth_voip outbound
d traffic-table name ftth_voip
```

3. 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
```

4. Save the data.

```
huawei(config)#save
```

● Configure the ONT 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 with the IP address of the local maintenance Ethernet port on the ONT (default: 192.168.100.1).
 - b. 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.
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 1-22 shows the parameter settings.

Figure 1-22 Parameter settings on the Web page for the voice WAN interface

		New	Delete
	Connection Name	VLAN/Priority	Protocol Type
<input type="checkbox"/>	1_VOIP_R_VID_1001	1001/0	IPv4

Basic Information			
Enable Wan Connection:	<input checked="" type="checkbox"/>		
Encapsulation Mode:	<input checked="" type="radio"/> IPoE <input type="radio"/> PPPoE		
Protocol Type:	IPv4		
Mode:	Route WAN		
Service List:	VOIP		
Enable VLAN:	<input checked="" type="checkbox"/>		
VLAN ID:	300 <small>*(1-4094)</small>		
802.1p:	5		
IP Acquisition Mode:	<input type="radio"/> Static <input checked="" type="radio"/> DHCP <input type="radio"/> PPPoE		
Vendor ID:	<input type="text"/> <small>(The vendor ID must be 0 - 63 characters in length.)</small>		
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>			

- c. Click **Apply**.
3. Configure parameters for the SIP-based voice interface.
 - a. Choose **Voice > VoIP Basic Configuration**.
 - b. In the right pane, configure the parameters as follows:
 - Set **Proxy Server Address** to **200.200.200.200**.
 - Set **Home Domain** to **huawei.com**.
 - Set **Region** to **CN-China**.
 - Set **Signaling Port** to **1_VOIP_R_VID_300**.

 **NOTE**

- **Standby Server Address** must be set if dual-homing is configured.
- If you do not set **Media Port**, 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 service flows 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**.

Figure 1-23 shows the parameter settings.

Figure 1-23 Parameter settings on the Web page for the SIP-based voice interface

Outbound Proxy Address:	<input type="text"/>	(IP or Domain)
Outbound Proxy Port:	<input type="text" value="5060"/>	(0-65535)
Standby Outbound Proxy Address:	<input type="text"/>	(IP or Domain)
Standby Outbound Proxy Port:	<input type="text" value="5060"/>	(0-65535)
Primary Proxy Address:	<input type="text" value="200.200.200.200"/>	(IP or Domain)
Primary Proxy Port:	<input type="text" value="5060"/>	(0-65535)
Standby Proxy Address:	<input type="text"/>	(IP or Domain)
Standby Proxy Port:	<input type="text" value="5060"/>	(0-65535)
Home Domain:	<input type="text" value="huawei.com"/>	(IP or Domain)
Local Port:	<input type="text" value="5060"/>	*(0-65535)
Digitmap:	<input type="text" value="x.S x.#"/>	
Digitmap Match Mode:	<input type="text" value="Min"/>	
Registration Period:	<input type="text" value="600"/>	(Unit:s)(1~65534)
Region:	<input type="text" value="CN - China"/>	
Signaling Port:	<input type="text" value="2_VOIP_R_VID_300"/>	(Select the name of the WAN that will c messages.)
Media Port:	<input type="text"/>	(Select the name of the WAN that will c media port is same with signaling port when it is empty.)
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>		

- c. Click **Apply**.
4. Configure parameters for the SIP-based voice users.
 - a. Choose **Voice > VoIP Basic Configuration**.
 - b. In the **User Basic Parameters** window, set parameters for voice user 1 as follows:
 - Select **Enable User** to enable the voice user configuration.
 - Set **Register User Name** to **77730010**.
 - Set **Associated POTS** to **1**.
 - Set **Auth User Name** to **+8675577730010@huawei.com**.
 - Set **Password** to **iadtest1**.

In the right pane, 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 **Register User Name** to **77730020**.

- Set **Associated POTS** to **2**.
- Set **Auth User Name** to **+8675577730020@huawei.com**.
- Set **Password** to **iadtest2**.

Figure 1-24 shows the parameter settings.

Figure 1-24 Parameter settings on the Web page for SIP-based voice user 2

User Basic Parameters					
On this page, you can set the basic parameters for the voice users.					
					New Delete
	Sequence	Register User Name	Auth User Name	Password	Associated POTS
<input type="checkbox"/>	1	77730010	+8675577730010@huawei.com	*****	1
<input type="checkbox"/>	2	77730020	+8675577730020@huawei.com	*****	2

Enable User:

Register User Name: (Telephone Number)

Associated POTS:

Auth User Name: (The length must be between 0-64.)

Password: (The length must be between 0-64.)

Apply Cancel

- c. Click **Apply**.
5. (Optional) Configure routes.

You need to configure routes when the IP address of the ONT and that of the voice server are in different network segments.

 - a. Choose **Route > Default Route Configuration**.
 - b. Select **Enable Default Route** and set **WAN Name** to **1_VOIP_R_VID_300**.

Figure 1-25 shows the parameter settings.

Figure 1-25 Route parameter settings

Route > Default Route Configuration

On this page, you can configure the default route.

Enable Default Route:

WAN Name:

Apply Cancel

- c. Click **Apply**.
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 1-26 shows the parameter settings.

Figure 1-26 Voice service restart


Sequence	User Name(Telephone Number)	Associated POTS	User Status	Call Status
1	77730010	1	Up	Idle
2	77730020	2	Up	Idle

- Configure the ONT on the U2000.
 1. Log in to the U2000 and enable the FTP service.
 2. Configure the value-added service (VAS) configuration profile of the ONT.

NOTE

The window for configuring ONT VAS profiles varies with ONT versions, but the parameter configuration is the same. For details, see relevant ONT manuals.

- a. Choose **Configuration > Access Profile Management** from the main menu. In the window that is displayed, choose **PON Profile > ONT VAS Profile** from the navigation tree.
- b. Click the **General ONT VAS Profile** tab.
- c. Right-click in the list and choose **Add** from the shortcut menu.
- d. In the dialog box that is displayed, set the parameters.
 - Profile name: *HG8245*
 - Choose **General Para > WAN Device > WAN Interface 1 > WAN Connection** from the navigation tree. Right-click **WAN Connection** and choose **Add IP Connection** from the shortcut menu. Select **WAN IP Connection 1** and configure the following parameters:
 - WAN Enable: *Enable*
 - Connection Type: *Routed*
 - Vlan ID: *300*
 - Priority: *5*
 - Choose **General Para > Services > Voice Service > Voice Service 1 > Interface Configuration > Interface 1** from the navigation tree and configure the following parameters:
 - Signaling Protocol: *SIP*
 - Associate WAN Interface: *WANI*

- Choose **General Para > Services > Voice Service > Voice Service 1 > Interface Configuration > Interface 1 > SIP** from the navigation tree and configure the following parameters:
 - Proxy Server: *200.200.200.200*
 - Proxy Server Port: *5060*
 - Home Domain: *huawei.com*
 - Choose **General Para > Services > Voice Service > Voice Service 1 > Interface Configuration > Interface 1 > User** from the navigation tree and select the **User** node.
 - Click **User 1**. Set **User Enabled** to **Enabled** and **Interface ID** to **1**, indicating that the TEL1 port on the ONT is bound.
 - Click **User 2**. Set **User Enabled** to **Enabled** and **Interface ID** to **2**, indicating that the TEL2 port on the ONT is bound.
 - Choose **General Para > Services > Voice Service > Voice Service 1 > Physical Interface** from the navigation tree. Right-click **Physical Interface** and choose **Add Physical Interface** from the shortcut menu.
 - Click **Next**.
 - In the dialog box that is displayed, set **vendor ID** to **HWTC**, **Terminal Type** to **HG8245**, and **Version** to **V1R002C06-V1R002Czz**. Then click **Add**.
 - In the dialog box that is displayed, set the parameters.
 - Choose **HG8245 Config Info > Services > Voice Service > Voice Service 1 > Interface Configuration > Interface 1** from the navigation tree. Set **Region** to **China**.
 - Choose **HG8245 Config Info > WAN Device > WAN Device 1 > WAN Connection > WAN Connection 1** from the navigation tree. Set **WAN Interface Name** to **ONT-VOIP**, **NATEnabled** to **Enable**, and **Service Type** to **VOIP**.
3. Bind the VAS profile and configure value-added services.
- a. Choose **GPON > GPON Management** from the navigation tree.
 - b. On the **GPON ONU** tab, enter the search criteria or click  to query the GPON ONU records.
 - c. Right-click an ONT record in the list and choose **Bind General VAS Profile** from the shortcut menu.
 - d. In the dialog box that is displayed, select the VAS profile with **Profile Name** being **HG8245** and click **OK**.
 - e. Right-click the ONT record and choose **Configure Value-Added Service** from the shortcut menu.
 - f. In the dialog box that is displayed, set the parameters.
On the **Basic Parameters** tab, select **Voice Service**.
 - Set **Auth User Name** to **+8675577730010@huawei.com**, **Directory Number** to **77730010**, and **Password** to **iadtest1** for **Interface ID 1**.
 - Set **Auth User Name** to **+8675577730020@huawei.com**, **Directory Number** to **77730020**, and **Password** to **iadtest2** for **Interface ID 2**.

g. Click **OK**.

----End

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.

Data Plan

Table 1-37 Data plan

Item	Data
ONT line profile	Profile name: fthh T-CONT ID: 4 GEM port ID: 12
ONT service profile	Profile name: fthh ONT port capability set: adaptive
Voice parameter	IP address of the SIP server: 200.200.200.200/24 Port ID of the SIP server: 5060 User phone number 1: 77730010 User phone number 2: 77730020

Prerequisite

- Data has been configured on the SIP server for interoperating with the SIP interface on the ONT.
- The connection between the OLT and the SIP server has been 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 [Adding an ONT to an OLT](#).
- The ONT software needs to support the configuration. Currently, only V100R002C02 supports this configuration.

Procedure

Step 1 Configure a VLAN translation policy and service flows.

1. Perform this step in the **gateway ONT (single VLAN tag)** scenario.

Table 1-38 Scenario plan

Scenario	VLAN Plan	VLAN Translation Policy
Scenario 1	Single VLAN tag <ul style="list-style-type: none"> ● 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 <ul style="list-style-type: none"> ● 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 ftt
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 gempport 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 gempport 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 ftt
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
outbound
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
outbound
d traffic-table name ftth_voip
```

Step 2 (Optional) Configure global media attributes.

Set the fax mode to transparent transmission and the maximum jitter buffer to 200 ms. Use default values for other parameters.

```
huawei(config)#ont-voip-media attribute faxmode passthru jitter-buffer max 200
```

Step 3 Configure the IP addresses of ONT SIP users.

```
huawei(config)#interface gpon 0/1
huawei(config-if-gpon-0/1)#ont ipconfig 1 1 static ip-address 10.10.10.10 mask
255.255.255.0 vlan 20
huawei(config-if-gpon-0/1)#ont ipconfig 1 2 static ip-address 10.10.10.20 mask
255.255.255.0 vlan 20
huawei(config-if-gpon-0/1)#quit
```

Step 4 Configure ONT voice service profiles.

The ONT voice service profiles include the digitmap profile, SIP agent profile, and POTS profile.

- The digitmap profile contains the digitmap information of the ONT, including the digitmap format and timeout time of the digitmap timer.
- The SIP agent profile contains the SIP agent information of the ONT, including the SIP agent server, signaling transmission mode, and signaling transmission port.
- The POTS profile contains the physical attributes of POTS ports on the ONT, including the port impedance and port signaling type.

1. Configure a digitmap profile.

Run the **display ont-digitmap-profile** command to query the existing digitmap profiles in the system. If the existing digitmap profiles in the system do not meet the requirements, run the **ont-digitmap-profile add** command to add a digitmap profile.

Create digitmap profile 2 with the internal digitmap format of the ONT.

```
huawei(config)#ont-digitmap-profile add profile-id 2 digitmap-format
not_defined
```

2. Configure a SIP agent profile.

Run the **display ont-sipagent-profile** command to query the existing SIP agent profiles in the system. If the existing SIP agent profiles do not meet the requirements, run the **ont-sipagent-profile add** command to add a SIP agent profile.

Create SIP agent profile 2, set the IP address of the SIP server to 200.200.200.200 and signaling port ID to 5060, and use default values for other parameters.

```
huawei(config)#ont-sipagent-profile add profile-id 2 proxy-server
200.200.200.200 signal signal-port 5060
```

3. Configure a POTS profile.

Run the **display ont-pots-profile** command to query the existing POTS profiles in the system. If the existing POTS profiles in the system do not meet the requirements, run the **ont-pots-profile add** command to add a POTS profile.

In this example, the default POTS profile, namely POTS port 1 is used.

Step 5 Configure SIP PSTN users.

1. Add PSTN users.

Add PSTN user **huawei1** (phone number: 77730010) and PSTN user **huawei2** (phone number: 77730020) on ONT1 and ONT2 respectively.

```
huawei (config) #interface gpon 0/1
huawei (config-if-gpon-0/1) #sippstnuser add 1 1 1 username huawei1 telno
77730010
huawei (config-if-gpon-0/1) #sippstnuser add 1 2 1 username huawei2 telno
77730020
```

2. Bind ONT voice service profiles to PSTN users.

The ONT voice service profiles include the digitmap profile, SIP agent profile, and POTS profile. By default, a new PSTN user is bound to SIP agent profile 1, digitmap profile 1, and POTS profile 1. If the default profiles do not meet the requirements, bind other profiles.

In this example, bind digitmap profile 2 and SIP agent profile 2 to the PSTN user. Use the default POTS profile.

```
huawei (config-if-gpon-0/1) #sippstnuser digitmap 1 1 1 digitmap-profile profile-
id 2
huawei (config-if-gpon-0/1) #sippstnuser digitmap 1 2 1 digitmap-profile profile-
id 2
huawei (config-if-gpon-0/1) #sippstnuser ipconfig 1 1 1 sip-agent-profile
profile-id 2
huawei (config-if-gpon-0/1) #sippstnuser ipconfig 1 2 1 sip-agent-profile
profile-id 2
huawei (config-if-gpon-0/1) #quit
```

Step 6 Save the data.

```
huawei (config) #save
```

----End

Result

After two telephone sets are connected to two POTS ports on different ONTs, calls can be made between the two telephone sets.

Configuring the Bridge WAN Multicast 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 license for the multicast program or the multicast user has already been requested and installed.
- The iTMS has configured the multicast VLAN (MVLAN) for IPTV WAN ports on the ONT, and the multicast VLAN is the same as the network-side MVLAN.
- 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 [Adding an ONT to an OLT](#).

Data Plan

Table 1-39 Data plan

Item	Data
ONT line profile	Profile name: fthh T-CONT ID: 4 GEM port ID: 13
ONT service profile	Profile name: fthh ONT 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

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 VLAN and service flows.

Table 1-40 Data plan

VLAN Plan	VLAN Translation Policy
Single VLAN tag <ul style="list-style-type: none"> ● SVLAN ID: 1000 ● VLAN type: smart ● VLAN attribute: common 	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.

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 fthh
huawei(config-gpon-lineprofile-1)#gem mapping 13 2 vlan 1000
huawei(config-gpon-lineprofile-1)#commit
huawei(config-gpon-lineprofile-1)#quit
```

Configure a VLAN translation policy for the Ethernet port on the ONT. If the ONT is connected to the STB through Ethernet port 2, the multicast forwarding mode is VLAN tag.

```
huawei(config)#ont-srvprofile gpon profile-name fthh
huawei(config-gpon-srvprofile-1)#multicast-forward tag
huawei(config-gpon-srvprofile-1)#port vlan eth 2 vlan 1000
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
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 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
```

9. Save the data.

```
huawei(config)#save
```

Step 2 The ONT does not need to be configured.

----End

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 multicast VLAN for IPTV WAN ports on the ONT, and the multicast VLAN is the same as the planned CVLAN.
- 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 [Adding an ONT to an OLT](#).

Data Plan

Table 1-41 Data plan

Item	Data
ONT line profile	Profile name: fth T-CONT ID: 4 GEM port ID: 13
ONT service profile	Profile name: fth ONT 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 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 VLAN and service flows.

Table 1-42 Data plan

VLAN Plan	VLAN Translation Policy
Single VLAN tag <ul style="list-style-type: none"> ● SVLAN ID: 1100 ● VLAN type: smart ● VLAN attribute: common ● CVLAN: 2001 	The ONT adds CVLAN tags (configured on the iTMS) to packets: untag<->C. The OLT implements VLAN translation: C<->S.

Configure the mapping relationship between a GEM port and a VLAN. The service flow of user VLAN 2001 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 2001
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 2001.

```
huawei(config)#ont-srvprofile gpon profile-name ftth
huawei(config-gpon-srvprofile-1)#port vlan eth 2 2001
huawei(config-gpon-srvprofile-1)#multicast-forward tag translation 2001
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 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 1100, and use traffic profile 8.

```
huawei(config)#service-port 3 vlan 1100 gpon 0/1/0 ont 1 gemport 13 multi-
service
user-vlan 2001 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 rx-cttr 8 tx-cttr 8
```

3. Save the data.

```
huawei(config)#save
```

Step 2 The ONT does not need to be configured.

----End

Configuring Link Aggregation, Congestion Control, and Security Policy

Service reliability is improved by configuring uplink aggregation and priority scheduling policy for upstream queues in global configuration mode, and service security is improved by configuring security policy in global configuration mode.

Background Information

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 [2.2.1 Security Design](#).

Procedure

- Configure link aggregation.

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.

According to "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 anti-DoS-attack.

1. Run the **security anti-dos enable** command to enable global anti-DoS attack.
2. Run the **security anti-dos control-packet policy** command to configure the policy of processing protocol packets when a DoS attack occurs.
3. Run the **security anti-dos control-packet rate** command to configure the threshold of the rate for sending protocol packets to the CPU.

- Enable anti-ICMP-attack.

Run the **security anti-icmpattack enable** command to enable anti-ICMP attack.

- Enable anti-IP-attack.

Run the **security anti-ipattack enable** command to enable anti-IP attack.

- Configure user security.

- Enable anti-MAC-duplicate.

Run the **security anti-macduplicate enable** command to enable anti-MAC-duplicate.

- Enable anti-IP spoofing.

The anti-IP spoofing function can be enabled or disabled at three levels. This anti-IP spoofing function takes effect only when it is enabled at all three levels.

1. Global level: Run the **security anti-ipspoofing enable** command in global configuration mode.
2. VLAN level: Run the **security anti-ipspoofing enable** command in VLAN service profile configuration mode.
3. Service port level: Run the **security anti-ipspoofing service-port serviceport-id enable** command.

- Configure service security.

- Enable DHCP Option82.

The DHCP option 82 function can be enabled or disabled at four levels. The DHCP option 82 function takes effect only when it is enabled at all four levels.

1. Global level: Run the **dhcp option82 enable** command in global configuration mode.
2. Port level: Run the **dhcp option82 port** or **dhcp option82 board** command to enable the function at the port level.
3. VLAN level: Run the **dhcp option82 enable** command in VLAN service profile configuration mode.
4. Service port level: Run the **dhcp option82 service-port** command.

- Enable PITP.

The PITP function can be enabled or disabled at four levels. The PITP function takes effect only when it is enabled at all four levels.

1. Global level: Run the **pitp enable pmode** command in global configuration mode.
2. Port level: Run the **pitp port** or **pitp board** command to enable the function at the port level.
3. VLAN level: Run the **pitp enable** command in VLAN service profile configuration mode.
4. Service port level: Run the **pitp service-port** command.

----End

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.	<ul style="list-style-type: none">● 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.	<ul style="list-style-type: none">● An ONT can simulate the caller or callee in a call to a phone. Only a functioning phone is required in the central equipment room.● An ONT supports a maximum of a call emulation.

Remote Service Verification Method	Function	Description
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 emulation 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>|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    : -
Emulator 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 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.
 - b. 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.
 - c. 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.
- 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 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      : 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 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.
 - a. Run the **display mac-address vlan** command to check the MAC address learning status of the voice service VLAN.
 - b. 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.
 - c. If the downstream port does not learn a MAC address, check whether the ONT is activated and whether physical links are normal.
 - d. 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.
 - e. If an IP address is allocated to the MAC address and there is a session border controller (SBC) on the network, log in to the SBC to check whether the voice service of the ONT is registered.
 - f. If the registration status is registering, check the voice configurations on the MGC/SIP server are consistent with those on the ONT. If there is no registration information, log in to the ONT onsite or remotely and check whether VoIP configurations are applied to 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
Command is being executed. Please wait...
Multicast flow statistic result: 8736(kbps)

----End

1.2.4 Configuring FTTH Triple Play Service in 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.

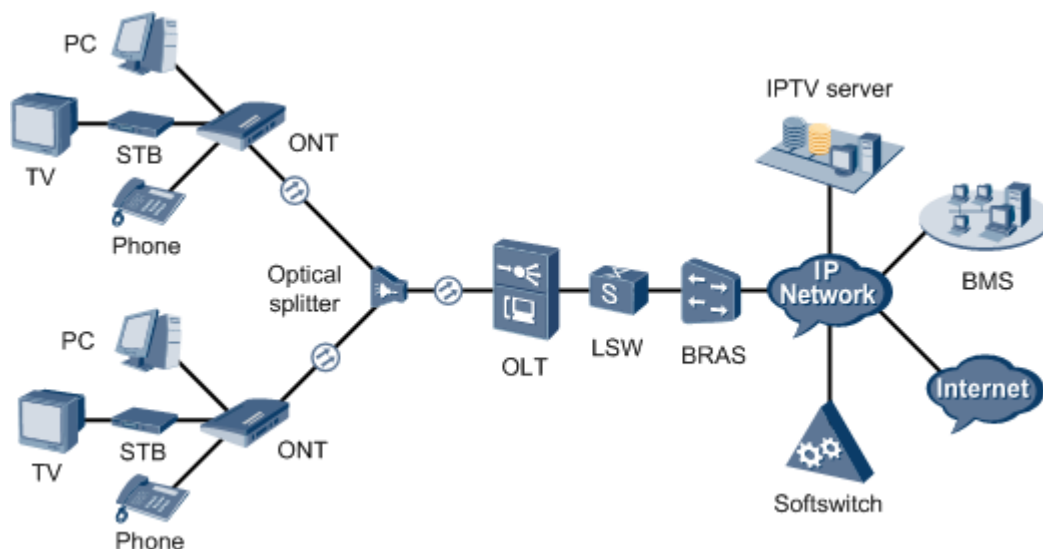
Service Requirements

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.
- The OLT in V800R008C05 can support configuring service ports in the simplified mode and services ports in the profile mode concurrently on the same ONT.
- 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 1-27 shows an example network of the FTTH triple play service.

Figure 1-27 Example network of the FTTH triple play service



Prerequisite

- The OLT is connected to the BRAS, MGC, and the multicast source.
- The interface data and the PSTN user 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.

```
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         :
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 VIAN 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.

```
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.



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 VIAN 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.

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
```

- 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 policy service-port 5 normal
huawei(config-btv)#igmp policy service-port 6 normal
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.
- The subscriber can watch program 1 on the TV.

2 Configuring the FTTB and FTTC Services

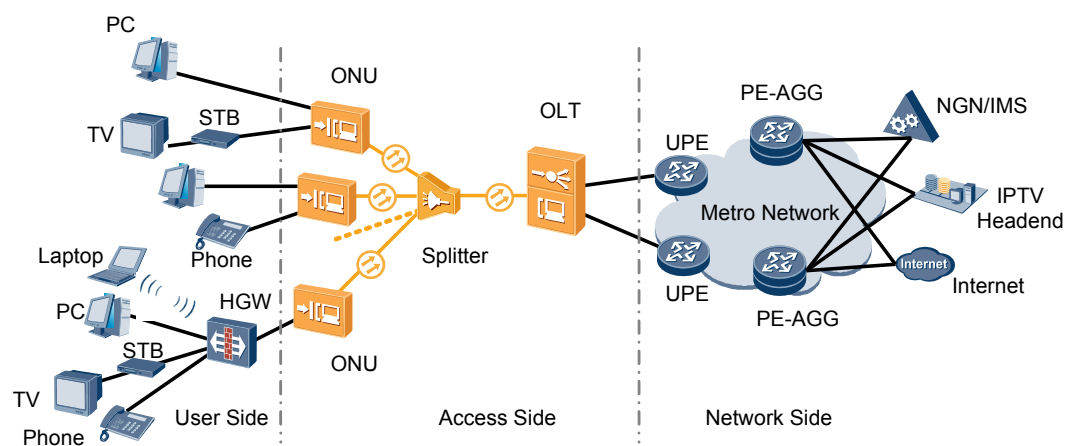
2.1 FTTB and FTTC Service Overview

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.

2.1.1 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



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 broadcast 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 MA5600Ts or MA5680Ts.
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 media distribution units (MDUs).
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.

Concept	Introduction
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.
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.

2.1.2 Scenario and Hardware Configuration

This topic describes typical FTTB and FTTC networking and their OLT and ONU hardware configurations based on analysis on location and model selection of ONUs, the key factor in FTTB and FTTC construction.

Typical FTTB and FTTC networking and hardware configurations

Scenario	Description	OLT Typical Configuration (Main Control Board + Service Board +Upstream Board)	MDU Configuration
FTTB Networking (LAN Access Without HGW)	<ul style="list-style-type: none"> ● 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. 	<ul style="list-style-type: none"> ● SCUN+GPBC/GPBD+GICF/GICG/X2CA 	ONUs applicable to this scenario: MA5620, MA5612, MA5616
FTTB/C Networking (xDSL Access Without HGW)	<ul style="list-style-type: none"> ● 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, MA5603T
FTTB +HGW Networking (ONU Providing the VoIP Service)	<ul style="list-style-type: none"> ● 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: MA5620, MA5612, MA5616, MA5603T. Among these ONUs, <ul style="list-style-type: none"> ● ONUs with LAN ports include MA5620, MA5612, MA5616. ● ONUs with xDSL ports include MA5616, MA5603T.

Scenario	Description	OLT Typical Configuration (Main Control Board + Service Board +Upstream Board)	MDU Configuration
FTTB +HGW Networking (HGW Providing the VoIP Service)	<ul style="list-style-type: none"> ● 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. 		<p>ONUs applicable to this scenario: MA5620, MA5626, MA5612, MA5616, MA5652, MA5662, MA5603T. Among these ONUs,</p> <ul style="list-style-type: none"> ● ONUs with LAN ports include MA5620, MA5626, MA5612, MA5616. ● ONUs with ADSL2+ ports include MA5616, MA5603T. ● ONUs with VDSL2 ports include MA5616, MA5652, MA5662, MA5603T.

2.1.3 GPON ONU Capability Sets

This topic describes the hardware capabilities, features, and positioning of GPON ONUs in FTTB and FTTC networks.

ONU Capability Sets

Table 2-1 shows the ONU capability sets provided by Huawei.

 **NOTE**

The **ONU Version Supported** column in **Table 2-1** lists only ONU versions supported for the FTTx V100R007.

Table 2-1 ONU capability sets

ONU Type	User Port	ONU Version Supported	Feature and Positioning
MA5620	<p>The MA5620 has the following specifications:</p> <ul style="list-style-type: none"> ● 1: 8 FE electrical ports+8 POTS ports ● 2: 16 FE electrical ports+16 POTS ports ● 3: 32 FE electrical ports+32 POTS ports 	<ul style="list-style-type: none"> ● V800R30 8C00 ● V800R31 0C00 	<p>It is mainly used in FTTB networks.</p>
MA5626	<p>The MA5626 has the following specifications:</p> <ul style="list-style-type: none"> ● 1: 8 FE electrical ports ● 2: 16 FE electrical ports ● 3: 24 FE electrical ports ● 4: 4 FE electrical ports+4 GE electrical ports (POE) ● 5: 8 FE electrical ports (inverse POE) 	<ul style="list-style-type: none"> ● V800R30 8C00 ● V800R31 0C00 	<p>It is mainly used in FTTB networks.</p>
MA5612	<p>The maximum number of ports depends on the service boards configured on the MA5612. RF ports are optional because some MA5612s do not support RF ports in their configurations.</p> <ul style="list-style-type: none"> ● Fully configured with two ASNB boards: 2 GE electrical ports+6 FE electrical ports+48 POTS ports+(optional) 1 RF port ● Fully configured with two EIUC boards: 2 GE electrical ports+22 FE electrical ports+16 POTS ports+(optional) 1 RF port ● Fully configured with two E81A boards: 2 GE electrical ports+6 FE electrical ports+16 E1/T1 ports+16 POTS ports+(optional) 1 RF port 	<ul style="list-style-type: none"> ● V800R30 8C00 ● V800R30 8C01 ● V800R31 0C00 	<p>It is mainly used in FTTB networks and some networks carrying private line access services.</p>

ONU Type	User Port	ONU Version Supported	Feature and Positioning
MA5616 (CCUB control board)	<ul style="list-style-type: none"> ● Fully configured with four ADPE boards: 256 ADSL2+ ports ● Fully configured with four VDLE boards: 128 VDSL2 ports ● Fully configured with four SHLH boards: 64 SHDSL ports ● Fully configured with four ASPB boards: 256 POTS ports ● Fully configured with four DSLD boards: 32 ISDN ports ● Fully configured with four CALE boards: 128 ADSL2+ ports+128 POTS ports 	<ul style="list-style-type: none"> ● V800R30 8C01 ● V800R30 9C00 ● V800R31 0C00 	It is mainly used in FTTB and FTTC networks.
MA5616 (CCUC control board)	<ul style="list-style-type: none"> ● Fully configured with four ADPE boards: 256 ADSL2+ ports ● Fully configured with four VDMM boards: 192 VDSL2 ports ● Fully configured with four SHLH boards: 64 SHDSL ports ● Fully configured with four ASPB boards: 256 POTS ports ● Fully configured with four EIUA boards: 64 FE ports ● Fully configured with four DSLD boards: 32 ISDN ports ● Fully configured with four CALE boards: 128 ADSL2+ ports+128 POTS ports ● Fully configured with two EIUD boards (only in slots 1 and 2): 8 GE optical ports (or 8 GE electrical ports)+8 FE optical ports 	<ul style="list-style-type: none"> ● V800R30 8C02 ● V800R30 9C00 ● V800R31 0C00 	
MA5652	<p>The MA5652 has the following specifications:</p> <ul style="list-style-type: none"> ● 1: 24 VDSL2 ports ● 2: 16 VDSL2 ports ● 3: 24 VDSL2 ports+1 RF port ● 4: 8 VDSL2 ports+1 RF port 	V800R310C00	It is mainly used in FTTB and FTTC networks.

ONU Type	User Port	ONU Version Supported	Feature and Positioning
MA5662	48 VDSL2 ports	<ul style="list-style-type: none"> ● V800R30 9C00 ● V800R31 0C00 	It is mainly used in FTTB and FTTC networks.
MA5603T	<ul style="list-style-type: none"> ● Fully configured with six ADPD/ADQD boards: 384 ADSL2+ ports ● Fully configured with six VDMF boards: 288 VDSL2 ports ● Fully configured with six SHLM boards: 96 ATM SHDSL/EFM SHDSL ports ● Fully configured with six H802EDTB boards: 96 TDM SHDSL ports ● Fully configured with six ASPB boards: 384 POTS ports ● Fully configured with six DSRD boards: 192 ISDN BRA ports ● Fully configured with six H801EDTB boards: 96 ISDN PRA ports 	V800R008C01	It is mainly used in FTTB and FTTC networks. FTTC networks account for over half of the total applications.

2.2 FTTB and FTTC Data Plan

This topic describes data plan for various FTTB and FTTC networking diagrams in terms of security, device management, QoS, and services. The examples in this topic are based on the planning data.

2.2.1 Security Design

Security design involves designs for system security, user security, and service security. 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	Suggestion	Configuration Method
DoS attack	Enable the anti-DoS-attack function.	After the anti-DoS-attack function is enabled, control packets are monitored and those exceeding the number threshold are discarded.	Use this solution in a new deployment.	<ol style="list-style-type: none"> 1. Run the security anti-dos enable command to enable global anti-DoS attack. 2. Run the security anti-dos control-packet policy command to configure the policy of processing protocol packets when a DoS attack occurs. 3. Run the security anti-dos control-packet rate command to configure the threshold of the rate for sending protocol packets to the CPU.
ICMP attack	Enable the anti-ICMP-attack function.	After the anti-ICMP-attack function is enabled, a device discards the ICMP 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 in a new deployment.	Run the security anti-icmpattack enable command to enable anti-ICMP attack.

Security Vulnerability	Solution	Description	Suggestion	Configuration Method
IP attack	Enable the anti-IP-attack function.	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 in a new deployment.	Run the security anti-ipattack enable command to enable anti-IP attack.

User Security

Security Vulnerability	Solution	Description	Suggestion	Configuration Method
MAC spoofing	Enable the anti-MAC-duplicate function.	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 in a new deployment.	Run the security anti-macduplicate enable command to enable anti-MAC-duplicate.

Security Vulnerability	Solution	Description	Suggestion	Configuration Method
IP spoofing	Enable the anti-IP spoofing function.	After the anti-IP spoofing is enabled, it can prevent users from forging IP addresses to perform malicious attacks.	Use this solution in a new deployment.	<p>The anti-IP spoofing function can be enabled or disabled at three levels. This anti-IP spoofing function takes effect only when it is enabled at all three levels.</p> <ol style="list-style-type: none"> 1. Global level: Run the security anti-ipspoofing enable command in global configuration mode. 2. VLAN level: Run the security anti-ipspoofing enable command in VLAN service profile configuration mode. 3. Service port level: Run the security anti-ipspoofing service-port <i>serviceport-id</i> enable command.

Service Security

Security Vulnerability	Solution	Description	Suggestion	Configuration Method
Unauthorized broadband access of small enterprises (IPoE)	DHCP option 82 is enabled on the access network, and the BRAS implements user authentication based on the RAIO information.	<p>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:</p> <ul style="list-style-type: none"> ● 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.	<p>The DHCP option 82 function can be enabled or disabled at four levels. The DHCP option 82 function takes effect only when it is enabled at all four levels.</p> <ol style="list-style-type: none"> 1. Global level: Run the dhcp option82 enable command in global configuration mode. 2. Port level: Run the dhcp option82 port or dhcp option82 board command to enable the function at the port level. 3. VLAN level: Run the dhcp option82 enable command in VLAN service profile configuration mode. 4. Service port level: Run the dhcp option82 service-port command.

Security Vulnerability	Solution	Description	Suggestion	Configuration Method
Broadband access of residential users (PPPoE), user account theft/borrowing	PPPoE+ (PITP) is enabled on the access network and the BRAS implements user authentication based on binding of RAIO to the user account.	<p>The BRAS responds to request packets of users with specified CID and RID. In this way, the following functions are implemented:</p> <ul style="list-style-type: none"> ● 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.	<p>The PITP function can be enabled or disabled at four levels. The PITP function takes effect only when it is enabled at all four levels.</p> <ol style="list-style-type: none"> 1. Global level: Run the pitp enable pmode command in global configuration mode. 2. Port level: Run the pitp port or pitp board command to enable the function at the port level. 3. VLAN level: Run the pitp enable command in VLAN service profile configuration mode. 4. Service port level: Run the pitp service-port command.

2.2.2 Device Management Data Plan

The device management plan includes channel management plan and the IP address plan.

Device Management Data Plan

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	Use a single S-VLAN as the equipment management VLAN of the ONU and that of all other equipment in the network.

Plan	Device/Service	Introduction
	HGW	Use a single S-VLAN as the management VLAN of the HGW that are managed by the Itms. 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).

2.2.3 QoS 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

Service Type	OLT				ONU		
	GEM port	Upstream			Downstream	Upstream	Downstream
		TCONT	DBA Type	DBA Bandwidth Planning	Traffic Profile	Port Rate Limit	Port Rate Limit
Management service	11	All services share a T-CONT.	Type 3 (DBA profile: assured bandwidth + maximum bandwidth. Users are allowed to preempt	Configure the DBA bandwidth according to the user's bandwidth package. The assured bandwidth	No rate limit	Set ONU port rate limit or xDSL line rate limit as required. [Remark 1]	Set ONU port rate limit or xDSL line rate limit as required. [Remark 1]
Internet access service	12				Configure rate limit by a traffic profile as required. [Remark 1]		

Service Type	OLT				ONU		
	GEM port	Upstream			Downstream	Upstream	Downstream
		TCON T	DBA Type	DBA Bandwidth Planning	Traffic Profile	Port Rate Limit	Port Rate Limit
VoIP service	13		the bandwidth on condition that the users' assured bandwidth is guaranteed. However, the total bandwidth cannot exceed the maximum bandwidth.)	th 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.	No rate limit		
IPTV service	14				No rate limit		

Remark 1: [Table 2-2](#) shows the reference service bandwidth of each service for each user.

Table 2-2 Reference Service Bandwidth of Each service for Each User

Service Type	Upstream Bandwidth	Downstream Bandwidth	Bandwidth Description
Internet access service	Determined based on the 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 transmitting IGMP packets, which requires little bandwidth and can be neglected.
IPTV service (high definition program)	/	9.7 Mbit/s channel	

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 GEM ports in the table are recommended value. GEM ports are arranged according to the operator's actual planning.
- 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.

2.2.4 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	
		ONU	OLT
FTTB networking (without HGWs)	Double-tagged VLAN (S-VLAN +C-VLAN)	The inner C-VLAN is mapped based on user port 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+HGW networking (ONU providing the VoIP service)		HGWs (LAN upstream transmission) <ul style="list-style-type: none"> ● Untagged upstream packets of HGWs: ONUs map C-VLANs based on user port. ● Tagged upstream packets of HGWs: ONUs translate user VLANs to C'-VLANs. [Remark 1] 	
FTTB+HGW networking (HGW providing the VoIP service)			

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.

TIP

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.

2.2.5 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 and VLAN translation policy

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.

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.

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			-
	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.

Item		Remarks
VoIP user 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: <ul style="list-style-type: none"> ● cat1: government1 (category 1 government users) ● cat2: government2 (category 2 government users) ● cat3: normal (common users). This is the default value.
	User type	According to the service requirements, user type needs to be specified. The user type includes the following: <ul style="list-style-type: none"> ● 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.

Item		Remarks
	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.
	Ring 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.

2.2.6 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.

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	Single - tagged VLAN	<p>1. The multicast VLAN (MVLAN) of the HGW is different from the network-side MVLAN.</p> <ul style="list-style-type: none"> 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 	<ul style="list-style-type: none"> 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.

Application Scenario	Service Type	VLAN Plan	VLAN Translation		Remarks
			ONU	OLT	
	VoD	Single-tagged VLAN	<p>VLAN translation policy:</p> <ul style="list-style-type: none"> 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.	<p>This solution is recommended.</p> <p>The PSPV mode is recommended for the VoD service because the service requires fewer VLANs.</p>

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 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.

Data Item	Remarks
IGMP version	<p>The compatibility policies of the IGMP version on access equipment distinguish between the network side and the user side.</p> <ol style="list-style-type: none"> 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. The terminals are always the active initiating party and can be seamlessly degraded without packet loss. <p>The recommended versions are as follows:</p> <ul style="list-style-type: none"> 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	<p>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.</p>
Multicast preview profile	Default
Multicast fast leave	Enabling this function is recommended. It reduced the exchange of IGMP packets, saving the bandwidth resources.

2.3 Configuring FTTB/FTTC Services in Various Scenarios

This topic describes how to configure the Internet access service, voice service and multicast service in GPON access mode in FTTB/FTTC networking scenarios.

Context

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	<pre> huawei (config) #diagnose huawei (diagnose) %%display xpon mode ----- Current config mode: Profile-mode ----- </pre>

Mode	Query Method
ADSL2+ common mode (RFC2662 mode)	huawei (config) # diagnose huawei (diagnose) %% display xdsl mode
VDSL2 common mode (TR129 mode)	----- ADSL Current mode : rfc2662 VDSL Current mode : tr129 -----

2.3.1 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.

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.

Considering simple and flexible service provisioning and easy OM, category-5 cables and FTTB (LAN access) are used for deployment.

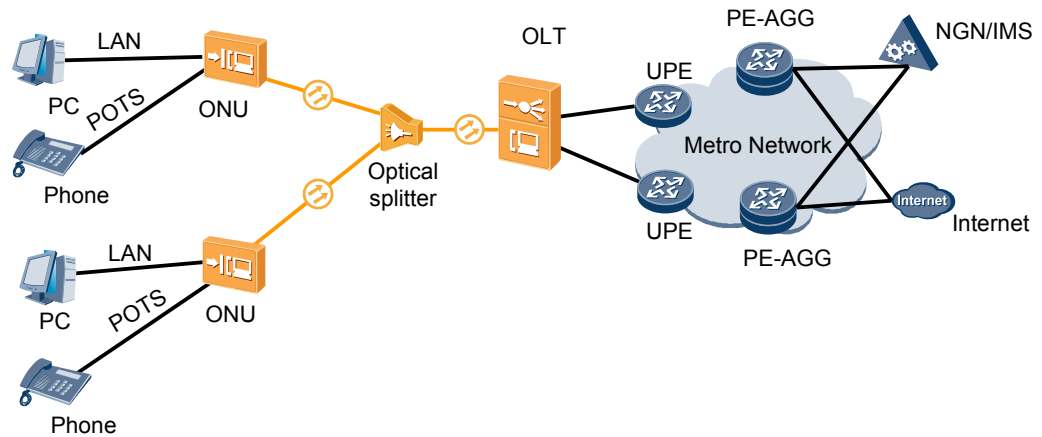
Application Scenarios

As shown in [Figure 2-1](#), 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: MA5620, MA5612, MA5616.

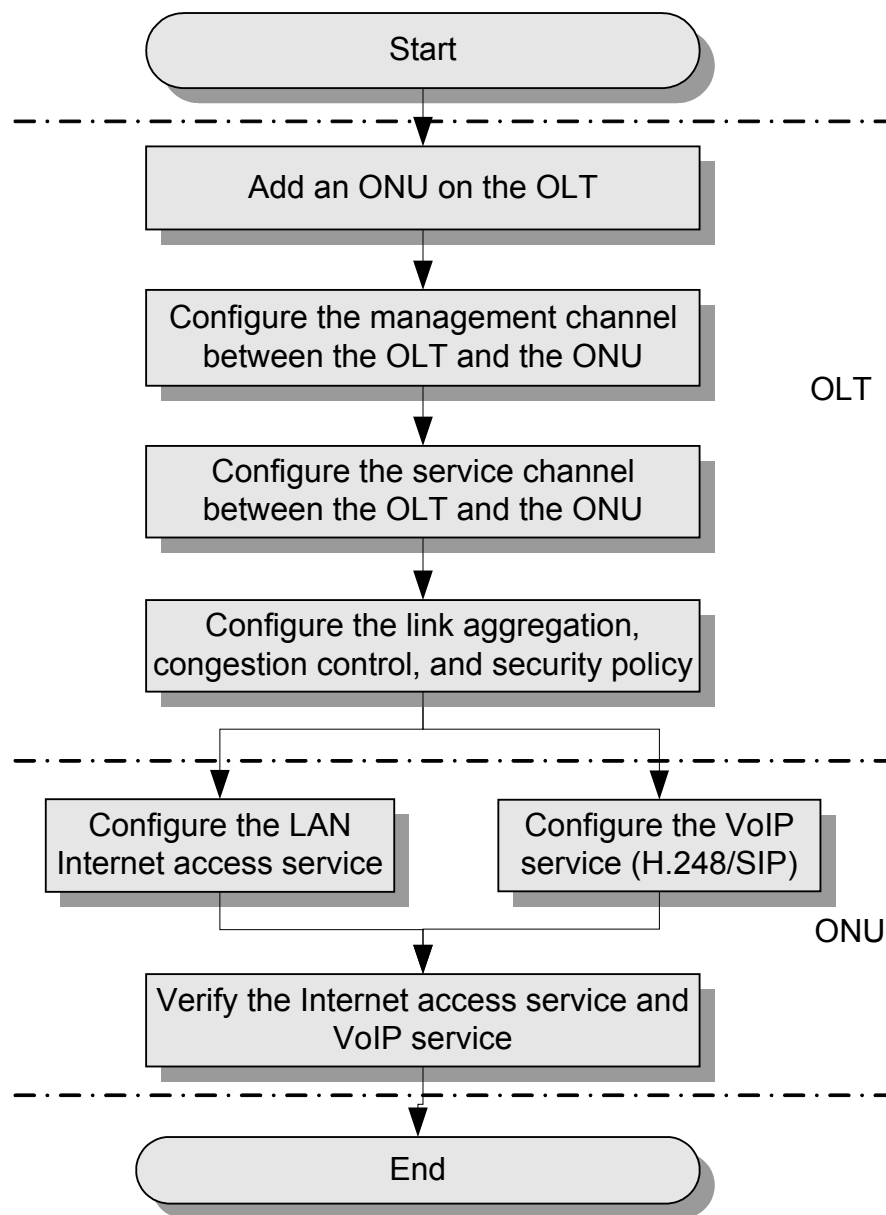
Figure 2-1 Example network of the FTTB service (LAN access)



Configuration Procedure

Figure 2-2 shows the configuration procedure in the FTTB and FTTC networking scenarios using LAN access without HGWs.

Figure 2-2 Configuration Procedure 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 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.

Item	Procedure		Remarks
	Configure the service channel between the OLT and the ONU.	<ul style="list-style-type: none"> ● 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.
	Configure the link aggregation, congestion control, and security policy.		Service reliability is improved by configuring uplink aggregation and priority scheduling policy for upstream queues in global config mode, and service security is improved by configuring security policy in global config mode.
ONU	Configure the LAN 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 (H.248/SIP).	Configure the H.248 VoIP service on the ONU. Configure the SIP 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.
	Verify the Internet access service and VoIP 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.

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 2-3](#).

Table 2-3 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.
Automatically discover 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 2-4 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 [2.2.3 QoS 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 802.1p priority. Map management service flows with 802.1p priority 6 to GEM port 11, Internet access service flows with 802.1p priority 0 to GEM port 12, and VoIP service flows with 802.1p priority 5 to GEM port 13.

```
huawei(config-gpon-lineprofile-10)#gem mapping 11 0 priority 6
huawei(config-gpon-lineprofile-10)#gem mapping 12 1 priority 0
huawei(config-gpon-lineprofile-10)#gem mapping 13 2 priority 5
```

- 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-epon-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.

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.

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 logging in to the MDU through telnet, 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 and the IP address to 192.168.50.1/24.

```
huawei(config)#vlan 8 smart
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, run the **telnet 192.168.50.2** command to telnet the ONU and then configure the ONU.

----End

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 2-5](#). Select either mode as required.

Table 2-5 Adding service flows

Mode	Command	Remarks
Add service flows one by one.	service-port	-

Mode	Command	Remarks
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.

Data plan

Item	Data	Remarks
Internet access service	<p>OLT VLAN ID:</p> <ul style="list-style-type: none"> ● 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 <p>Upstream VLANs of the ONU: 1001-1016</p> <p>Service flow ID: 101</p>	<p>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.</p> <p>For details about the data plan, see 2.2.4 Internet Access Service Data Plan.</p>
VoIP service	<p>OLT VLAN ID (VLAN transparently transmitting the ONU service): 200</p> <p>ONU VLAN ID: 200</p> <p>Service flow ID: 201</p>	<p>For details about the data plan, see 2.2.5 VoIP Service Data Plan.</p>

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  
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

Configuring Link Aggregation, Congestion Control, and Security Policy

Service reliability is improved by configuring uplink aggregation and priority scheduling policy for upstream queues in global config mode, and service security is improved by configuring security policy in global config mode.

Background Information

In link aggregation, multiple upstream Ethernet ports are aggregated into a group to increase bandwidth and reliability of OLT uplinks. You are advised to configure link aggregation.

In congestion control, queue scheduling is used to put packets from one port into multiple queues and then process the packets based on queue priorities. You are advised to configure congestion control.

Security policy involves system security, user security, and service security, ensuring normal services from different aspects.

 **NOTE**

You are advised to enable the service security feature according to service types. For details, see [2.2.1 Security Design](#).

Procedure

- Configure link 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. The working mode is LACP static aggregation.

```
huawei(config)#link-aggregation 0/19 0-1 ingress workmode lacp-static
```
- Configure queue scheduling.
According to "[2.2.3 QoS Plan](#)", all packets are scheduled in strict priority (SQ) 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 anti-DoS attack.
 1. Run the **security anti-dos enable** command to enable global anti-DoS attack.
 2. Run the **security anti-dos control-packet policy** command to configure the policy of processing protocol packets when a DoS attack occurs.
 3. Run the **security anti-dos control-packet rate** command to configure the threshold of the rate for sending protocol packets to the CPU.
 - Enable anti-ICMP attack.
Run the **security anti-icmpattack enable** command to enable anti-ICMP attack.
 - Enable anti-IP attack.
Run the **security anti-ipattack enable** command to enable anti-IP attack.
- Configure user security.
 - Enables anti-MAC transfer.
Run the **security anti-macduplicate enable** command to enable anti-MAC-duplicate.
 - Enable anti-IP spoofing.
The anti-IP spoofing function can be enabled or disabled at three levels. This anti-IP spoofing function takes effect only when it is enabled at all three levels.
 1. Global level: Run the **security anti-ipspoofing enable** command in global configuration mode.
 2. VLAN level: Run the **security anti-ipspoofing enable** command in VLAN service profile configuration mode.
 3. Service port level: Run the **security anti-ipspoofing service-port serviceport-id enable** command.
- Configure service security.
 - Enable DHCP option 82, which is used in DHCP dialup as recommended.

The DHCP option 82 function can be enabled or disabled at four levels. The DHCP option 82 function takes effect only when it is enabled at all four levels.

1. Global level: Run the **dhcp option82 enable** command in global configuration mode.
 2. Port level: Run the **dhcp option82 port** or **dhcp option82 board** command to enable the function at the port level.
 3. VLAN level: Run the **dhcp option82 enable** command in VLAN service profile configuration mode.
 4. Service port level: Run the **dhcp option82 service-port** command.
- Enable PITP, which is used in PPPoE dialup as recommended.

The PITP function can be enabled or disabled at four levels. The PITP function takes effect only when it is enabled at all four levels.

1. Global level: Run the **pitp enable pmode** command in global configuration mode.
2. Port level: Run the **pitp port** or **pitp board** command to enable the function at the port level.
3. VLAN level: Run the **pitp enable** command in VLAN service profile configuration mode.
4. Service port level: Run the **pitp service-port** command.

---End

Configuring LAN Internet Access Service (ONU Side)

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.

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 2.2.4 Internet Access Service Data Plan .

Item	Data	Remarks
Traffic profile	Profile ID: 8 Committed rate: 4 Mbit/s Priority: 0	For details about the data plan, see 2.2.3 QoS Plan .

Procedure

Step 1 Log in to and configure the ONU.

Log in to the ONU from the OLT by telnet the management IP address of the ONU. By default, 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.

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

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.



WARNING

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 [2.2.5 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	17.10.10.10/24
		Default gateway IP address	17.10.10.1/24
	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)		

Item		Data
Voice user 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.

Log in to the ONU from the OLT by telnet the management IP address of the ONU. By default, 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 IP address of the Layer 3 interface to 17.10.10.10

```
huawei (config) #interface vlanif 200  
huawei (config-if-vlanif200) #ip address 17.10.10.10 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 17.10.10.10 and the MG IP address to 17.10.10.1.

```
huawei (config) #voip  
huawei (config-voip) #ip address media 17.10.10.10 17.10.10.1
```

```
huawei(config-voip)#ip address signaling 17.10.10.10
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 17.10.10.1 to 200.200.200.0.

```
huawei(config)#ip route-static 200.200.200.0 24 17.10.10.1
```

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 17.10.10.10 mgport
2944 code text transfer udp primary-mgc-ip1 200.200.200.200 primary-mgc-port
2944 mg-media-ip1 17.10.10.10 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.

```
huawei(config)#save
```

----End

Configuring SIP Voice Service (on an 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.



WARNING

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 [2.2.5 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	17.10.10.10/24
		Default gateway IP address	17.10.10.1/24
	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 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.

Log in to the ONU from the OLT by telnet the management IP address of the ONU. By default, 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 IP address of the Layer 3 interface to 17.10.10.10

```
huawei (config) #interface vlanif 200
huawei (config-if-vlanif200) #ip address 17.10.10.10 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 17.10.10.10, and the media gateway to 17.10.10.1.

```
huawei (config) #voip
huawei (config-voip) #ip address media 17.10.10.10 17.10.10.1
huawei (config-voip) #ip address signaling 17.10.10.10
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 17.10.10.1 to the network segment 200.200.200.0.

```
huawei (config) #ip route-static 200.200.200.0 24 17.10.10.1
```

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 17.10.10.10 signal-ip
17.10.10.10 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.

```
huawei(config)#save
```

----End

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 dialup emulation	By emulating PPPoE terminal software, an ONU dials up and interacts with the BRAS, to verify the connectivity between the ONT and BRAS.	<p>PPPoE dialup emulation requires a service flow that does not belong to a QinQ VLAN.</p> <p>The user name, password, and authentication mode must be configured on the BRAS before the PPPoE dialup emulation starts.</p> <p>An ONU supports one line of emulated call.</p>
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.	<ul style="list-style-type: none"> ● An ONU can emulate a caller or callee in an emulation test. A functional phone is required in the test. ● An ONU can emulate the caller and callee simultaneously in an emulation test. No phone is required in the test. ● An ONU supports one line of emulated call.

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.

```
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 stop** 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

2.3.2 FTTB/C Scenario (xDSL Access, Without HGW)

In the Fiber-to-the-building/curb (FTTB/C) scenario, 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.

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.

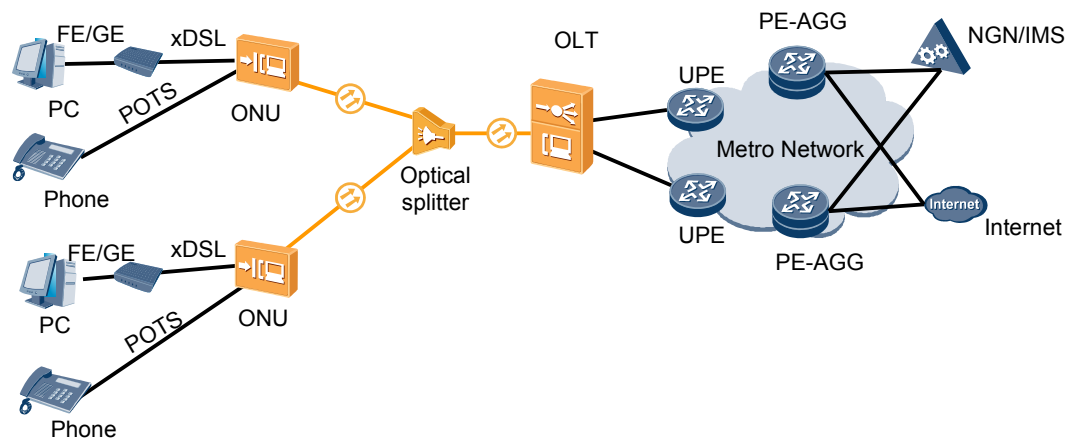
Application Scenario

As shown in [Figure 2-3](#), 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, MA5603T.

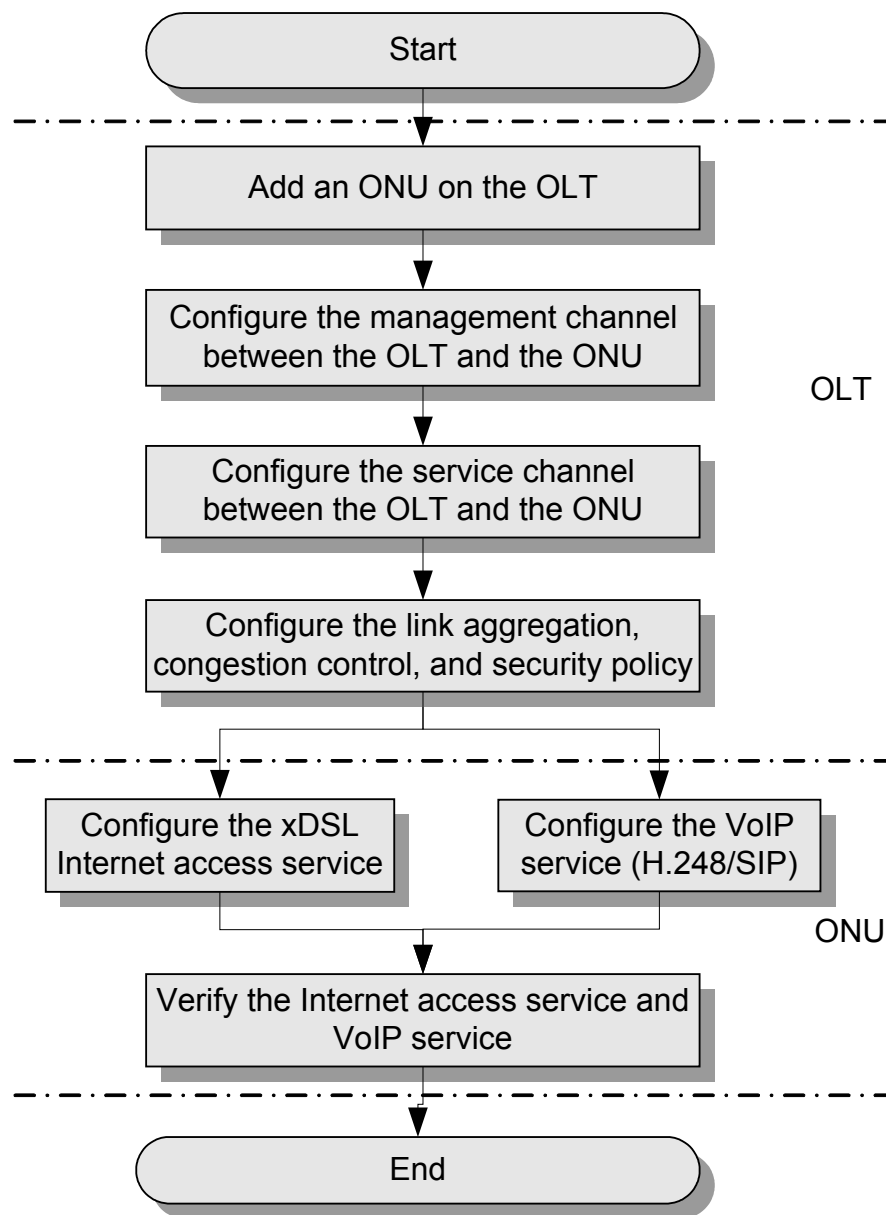
Figure 2-3 FTTB/C networking diagram (xDSL)



Configuration Procedure

[Figure 2-4](#) shows the configuration procedure in the FTTB and FTTC networking scenarios using xDSL access without HGWs.

Figure 2-4 Configuration Procedure in the FTTB and FTTC Networking Scenarios Using xDSL Access Without HGWs.



The following table lists the detailed description steps..

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.

Item	Procedure		Remarks	
	Configure the service channel between the OLT and the ONU.	<ul style="list-style-type: none"> ● 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.	
	Configure the link aggregation, congestion control, and security policy.		Service reliability is improved by configuring uplink aggregation and priority scheduling policy for upstream queues in global config mode, and service security is improved by configuring security policy in global config mode.	
ONU	Configure the Internet access service.	Configure the ADSL2+ Internet access service on the ONU.	NOTE Different ONUs have different ports, including ADSL2+ and VDSL2 ports, for the Internet access. Select a corresponding configuration method according to the port type.	
		Configure the ADSL2 Internet access service on the ONU.		
	Configure the VoIP service (H.248/SIP).	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.		
Verify the Internet access service and VoIP 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.		

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 2-6](#). Select either mode as required.

Table 2-6 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.

Data plan

Item	Data	Remarks
Internet access service	<p>OLT VLAN ID:</p> <ul style="list-style-type: none"> ● 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 <p>Upstream VLANs of the ONU: 1001-1016</p> <p>Service flow ID: 101</p>	<p>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.</p> <p>For details about the data plan, see 2.2.4 Internet Access Service Data Plan.</p>
VoIP service	<p>OLT VLAN ID (VLAN transparently transmitting the ONU service): 200</p> <p>ONU VLAN ID: 200</p> <p>Service flow ID: 201</p>	<p>For details about the data plan, see 2.2.5 VoIP Service Data Plan.</p>

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 gempport 12 multi-
service
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 gempport 13 multi-
service
user-vlan 200 rx-cttr 9 tx-cttr 9
```

---End

Configuring Link Aggregation, Congestion Control, and Security Policy

Service reliability is improved by configuring uplink aggregation and priority scheduling policy for upstream queues in global config mode, and service security is improved by configuring security policy in global config mode.

Background Information

In link aggregation, multiple upstream Ethernet ports are aggregated into a group to increase bandwidth and reliability of OLT uplinks. You are advised to configure link aggregation.

In congestion control, queue scheduling is used to put packets from one port into multiple queues and then process the packets based on queue priorities. You are advised to configure congestion control.

Security policy involves system security, user security, and service security, ensuring normal services from different aspects.

NOTE

You are advised to enable the service security feature according to service types. For details, see [2.2.1 Security Design](#).

Procedure

- Configure link 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. The working mode is LACP static aggregation.

```
huawei(config)#link-aggregation 0/19 0-1 ingress workmode lACP-static
```
- Configure queue scheduling.
According to "[2.2.3 QoS Plan](#)", all packets are scheduled in strict priority (SQ) 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 anti-DoS attack.
 1. Run the **security anti-dos enable** command to enable global anti-DoS attack.
 2. Run the **security anti-dos control-packet policy** command to configure the policy of processing protocol packets when a DoS attack occurs.
 3. Run the **security anti-dos control-packet rate** command to configure the threshold of the rate for sending protocol packets to the CPU.
 - Enable anti-ICMP attack.
Run the **security anti-icmpattack enable** command to enable anti-ICMP attack.
 - Enable anti-IP attack.
Run the **security anti-ipattack enable** command to enable anti-IP attack.
- Configure user security.
 - Enables anti-MAC transfer.
Run the **security anti-macduplicate enable** command to enable anti-MAC-duplicate.
 - Enable anti-IP spoofing.
The anti-IP spoofing function can be enabled or disabled at three levels. This anti-IP spoofing function takes effect only when it is enabled at all three levels.

1. Global level: Run the **security anti-ipspoofing enable** command in global configuration mode.
 2. VLAN level: Run the **security anti-ipspoofing enable** command in VLAN service profile configuration mode.
 3. Service port level: Run the **security anti-ipspoofing service-port *serviceport-id* enable** command.
- Configure service security.
 - Enable DHCP option 82, which is used in DHCP dialup as recommended.

The DHCP option 82 function can be enabled or disabled at four levels. The DHCP option 82 function takes effect only when it is enabled at all four levels.

 1. Global level: Run the **dhcp option82 enable** command in global configuration mode.
 2. Port level: Run the **dhcp option82 port** or **dhcp option82 board** command to enable the function at the port level.
 3. VLAN level: Run the **dhcp option82 enable** command in VLAN service profile configuration mode.
 4. Service port level: Run the **dhcp option82 service-port** command.
 - Enable PITP, which is used in PPPoE dialup as recommended.

The PITP function can be enabled or disabled at four levels. The PITP function takes effect only when it is enabled at all four levels.

 1. Global level: Run the **pitp enable pmode** command in global configuration mode.
 2. Port level: Run the **pitp port** or **pitp board** command to enable the function at the port level.
 3. VLAN level: Run the **pitp enable** command in VLAN service profile configuration mode.
 4. Service port level: Run the **pitp service-port** command.

---End

Configuring the Internet Access Service (ADSL2+ Access, ONU Side)

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.

Background Information

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 2-7](#).

Table 2-7 ADSL2+ profile

Profile Type	Function	Configuration
ADSL2+ line profile	<p>An ADSL2+ line profile provides the following parameters:</p> <ul style="list-style-type: none"> ● ADSL/ADSL2+ working mode ● Channel mode ● Upstream/Downstream line rate ● Upstream/Downstream interleave depth ● Noise margin <p>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.</p>	<p>The system has four default profiles (profile 1, profile 1022, profile 1023, and profile 1024) for activation of ADSL2+ ports in different conditions.</p> <ul style="list-style-type: none"> ● 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. <p>Commands:</p> <ul style="list-style-type: none"> ● To query: display adsl line-profile ● To add: adsl line-profile add or adsl line-profile quickadd
ADSL2+ alarm profile	<p>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.</p>	<p>Commands:</p> <ul style="list-style-type: none"> ● 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	<p>ID: 8</p> <p>CIR: 4 Mbit/s</p> <p>VLAN priority: 0</p> <p>Downstream priority policy: local-setting</p>	A traffic profile implements rate-limiting.
VPI/VCI of ADSL2+ users	<p>VPI: 0</p> <p>VCI: 35</p>	Internet service providers (ISPs) provide VPI/VCI information.

Item	Data	Remarks
ADSL2+ line profile	ID: 1024 (default); key parameters: <ul style="list-style-type: none">● 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.

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).

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.

As packets from HGWs contain VPI/VCI information, the PVC needs to be mapped to the user VLAN when a service flow is configured.

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.

- 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

Configuring the Internet Access Service (VDSL2 Access, ONU Side)

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.

Background Information

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 2-8](#).

Table 2-8 VDSL2 template

Templ ate 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.	<p>The system has one default VDSL2 line template (template 1), which is used for activation of common VDSL2 ports.</p> <ul style="list-style-type: none"> ● 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).	<ul style="list-style-type: none"> ● To query: display vdsl line-profile ● To add: vdsl line-profile add or vdsl line-profile quickadd

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.	<ul style="list-style-type: none"> ● 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.	<p>The system has one default VDSL2 alarm template (template 1).</p> <ul style="list-style-type: none"> ● To query: display vdsl alarm-template ● To add: vdsl alarm-template add or vdsl alarm-template quickadd
	<p>A VDSL2 line alarm profile provides the following parameters for COs and CPEs:</p> <ul style="list-style-type: none"> ● 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 	<ul style="list-style-type: none"> ● To query: display vdsl alarm-profile ● To add: vdsl alarm-profile add or vdsl alarm-profile quickadd
	<p>A VDSL2 channel alarm profile provides the following parameters for COs and CPEs:</p> <ul style="list-style-type: none"> ● Coding violations counts (CVC) ● Corrected blocks counts (CBC) 	<ul style="list-style-type: none"> ● To query: display vdsl channel-alarm-profile ● To add: vdsl channel-alarm-profile add or vdsl channel-alarm-profile quickadd

Data Plan

Table 2-9 provides key information about the Internet access service (VDSL2 access).

Table 2-9 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. <ul style="list-style-type: none"> ● 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.

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).

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 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

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.



WARNING

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 [2.2.5 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	17.10.10.10/24
		Default gateway IP address	17.10.10.1/24
	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 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.

Log in to the ONU from the OLT by telnet the management IP address of the ONU. By default, 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 IP address of the Layer 3 interface to 17.10.10.10

```
huawei (config) #interface vlanif 200
huawei (config-if-vlanif200) #ip address 17.10.10.10 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 17.10.10.10 and the MG IP address to 17.10.10.1.

```
huawei (config) #voip
huawei (config-voip) #ip address media 17.10.10.10 17.10.10.1
huawei (config-voip) #ip address signaling 17.10.10.10
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 17.10.10.1 to 200.200.200.0.

```
huawei (config) #ip route-static 200.200.200.0 24 17.10.10.1
```

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 17.10.10.10 mgport
2944 code text transfer udp primary-mgc-ip1 200.200.200.200 primary-mgc-port
2944 mg-media-ip1 17.10.10.10 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.

```
huawei(config)#save
```

----End

Configuring SIP Voice Service (on an 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.



WARNING

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 [2.2.5 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	17.10.10.10/24
		Default gateway IP address	17.10.10.1/24
	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

Item	Data	
	Home domain name (SIP)	huawei
	Profile index (SIP)	1
Voice user 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.

Log in to the ONU from the OLT by telnet the management IP address of the ONU. By default, 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 IP address of the Layer 3 interface to 17.10.10.10

```
huawei(config)#interface vlanif 200
huawei(config-if-vlanif200)#ip address 17.10.10.10 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 17.10.10.10, and the media gateway to 17.10.10.1.

```
huawei(config)#voip
huawei(config-voip)#ip address media 17.10.10.10 17.10.10.1
```

```
huawei(config-voip)#ip address signaling 17.10.10.10
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 17.10.10.1 to the network segment 200.200.200.0.

```
huawei(config)#ip route-static 200.200.200.0 24 17.10.10.1
```

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 17.10.10.10 signal-ip
17.10.10.10 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.

```
huawei(config)#save
```

----End

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 one line of emulated call.
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.	<ul style="list-style-type: none">● An ONU can emulate a caller or callee in an emulation test. A functional phone is required in the test.● An ONU can emulate the caller and callee simultaneously in an emulation test. No phone is required in the test.● An ONU supports one line of emulated call.

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.

```
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

2.3.3 FTTB+HGW Scenario (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.

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

As shown in [Figure 2-5](#), 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.

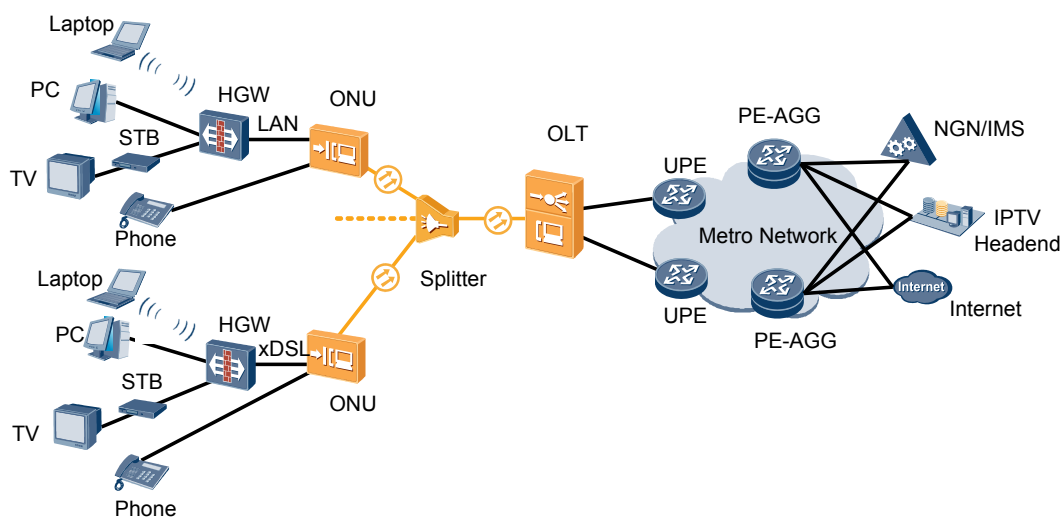
- An HGW sends services upstream to an ONU through ETH or xDSL ports, and provides Internet services for downstream subscribers through fast Ethernet (FE) ports or WiFi, and IPTV services through FE ports.
- The HGW has Layer 3 functions (such as PPPoE dialup and NAT), which enable multiple PCs of a 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 MA5620, MA5612, MA5616, MA5603T.

- LAN ports are available on MA5620, MA5612, MA5616.
- xDSL ports are available on MA5616, MA5603T.

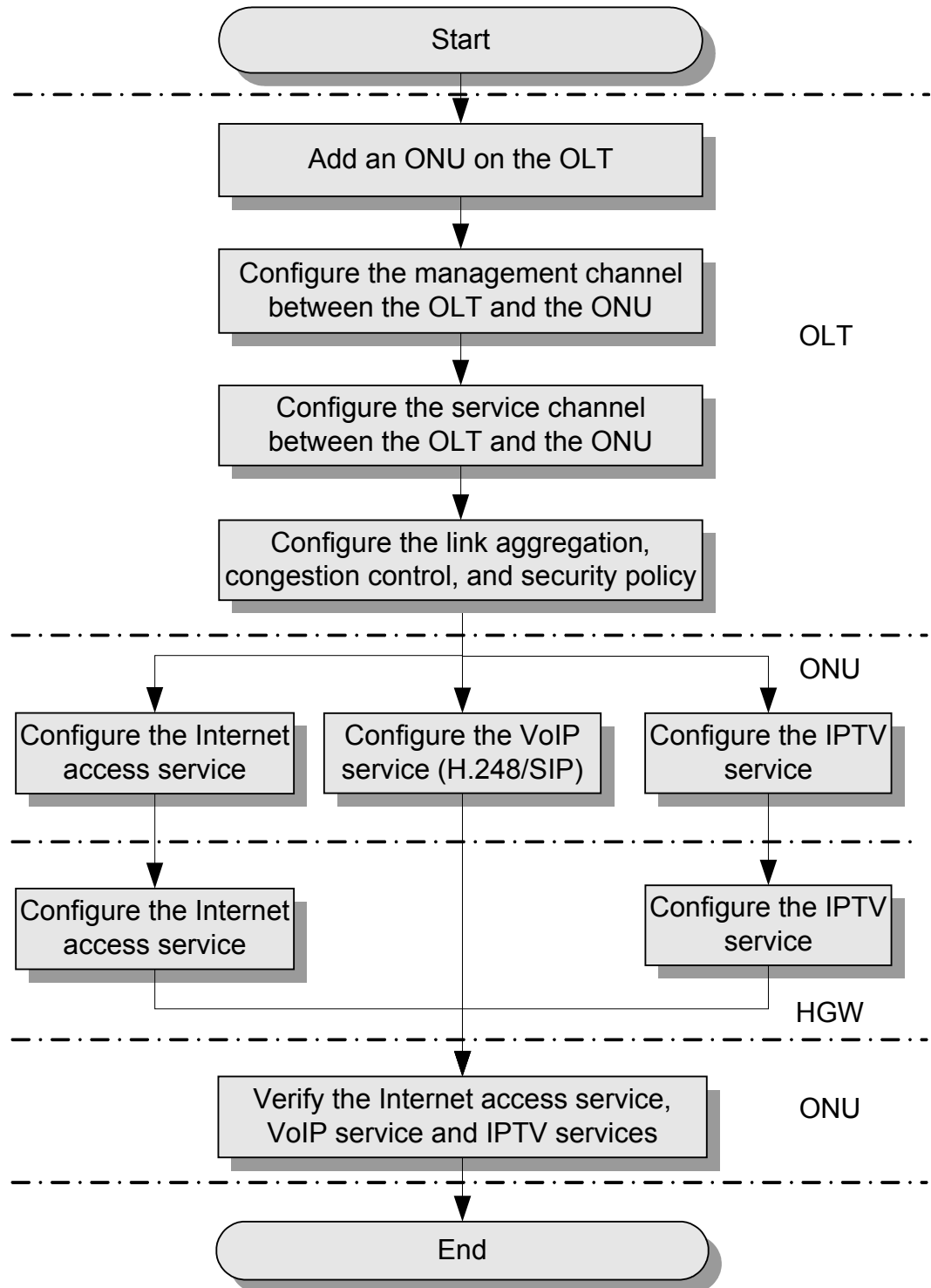
Figure 2-5 GPON FTTB+HGW networking Diagram (voice, Internet access and IPTV services)



Configuration Procedure

Figure 2-6 shows the configuration procedure in the FTTB+HGW networking scenarios (ONU providing the VoIP service).

Figure 2-6 Configuration Procedure in the FTTB+HGW Networking Scenarios (ONU Providing the VoIP Service)



The following table lists the detailed description steps..

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 from the OLT to 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 management channel from the OLT to the ONU.	<ul style="list-style-type: none"> ● Configure the Internet access service channel. ● Configuring the VoIP service channel. ● Configure the VoD service channel ● Configuring the multicast service channel. 	In the FTTB+HGW networking (ONU providing 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.
	Configure the link aggregation, congestion control, and security policy.		Service reliability is improved by configuring uplink aggregation and priority scheduling policy for upstream queues in global config mode, and service security is improved by configuring security policy in global config mode.
ONU	Configure the Internet access service.	Configure the LAN Internet access service on the ONU.	NOTE Different ONUs have different ports, including LAN, ADSL2+ and VDSL2 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 ADSL2 Internet access service on the ONU.	

Item	Procedure		Remarks
	Configure the VoIP service (H.248/SIP).	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.	
	Configure the IPTV service.	<ul style="list-style-type: none"> ● Configure the VoD service. ● Configure the multicast service. 	The IPTV service includes the VoD and multicast services that are different in configuration procedures and need to be configured separately.
HGW	Configuring 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 that uses ADSL2+ for upstream transmission as examples.
	Configure the IPTV service on the HGW.		-
ONU	Verify the Internet access service, VoIP service and IPTV 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.

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. **Adding an ONU to an OLT** is performed.
2. **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.

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 2.2.4 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 2.2.5 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 2.2.6 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 2.2.6 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.

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 default 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.

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.

```
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

Configuring Link Aggregation, Congestion Control, and Security Policy

Service reliability is improved by configuring uplink aggregation and priority scheduling policy for upstream queues in global config mode, and service security is improved by configuring security policy in global config mode.

Background Information

In link aggregation, multiple upstream Ethernet ports are aggregated into a group to increase bandwidth and reliability of OLT uplinks. You are advised to configure link aggregation.

In congestion control, queue scheduling is used to put packets from one port into multiple queues and then process the packets based on queue priorities. You are advised to configure congestion control.

Security policy involves system security, user security, and service security, ensuring normal services from different aspects.

NOTE

You are advised to enable the service security feature according to service types. For details, see [2.2.1 Security Design](#).

Procedure

- Configure link 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. The working mode is LACP static aggregation.

```
huawei(config)#link-aggregation 0/19 0-1 ingress workmode lacp-static
```
- Configure queue scheduling.
According to "[2.2.3 QoS Plan](#)", all packets are scheduled in strict priority (SQ) 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 anti-DoS attack.
 1. Run the **security anti-dos enable** command to enable global anti-DoS attack.
 2. Run the **security anti-dos control-packet policy** command to configure the policy of processing protocol packets when a DoS attack occurs.
 3. Run the **security anti-dos control-packet rate** command to configure the threshold of the rate for sending protocol packets to the CPU.
 - Enable anti-ICMP attack.

- Run the **security anti-icmpattack enable** command to enable anti-ICMP attack.
- Enable anti-IP attack.
Run the **security anti-ipattack enable** command to enable anti-IP attack.
 - Configure user security.
 - Enables anti-MAC transfer.
Run the **security anti-macduplicate enable** command to enable anti-MAC-duplicate.
 - Enable anti-IP spoofing.
The anti-IP spoofing function can be enabled or disabled at three levels. This anti-IP spoofing function takes effect only when it is enabled at all three levels.
 1. Global level: Run the **security anti-ipspoofing enable** command in global configuration mode.
 2. VLAN level: Run the **security anti-ipspoofing enable** command in VLAN service profile configuration mode.
 3. Service port level: Run the **security anti-ipspoofing service-port serviceport-id enable** command.
 - Configure service security.
 - Enable DHCP option 82, which is used in DHCP dialup as recommended.
The DHCP option 82 function can be enabled or disabled at four levels. The DHCP option 82 function takes effect only when it is enabled at all four levels.
 1. Global level: Run the **dhcp option82 enable** command in global configuration mode.
 2. Port level: Run the **dhcp option82 port** or **dhcp option82 board** command to enable the function at the port level.
 3. VLAN level: Run the **dhcp option82 enable** command in VLAN service profile configuration mode.
 4. Service port level: Run the **dhcp option82 service-port** command.
 - Enable PITP, which is used in PPPoE dialup as recommended.
The PITP function can be enabled or disabled at four levels. The PITP function takes effect only when it is enabled at all four levels.
 1. Global level: Run the **pitp enable pmode** command in global configuration mode.
 2. Port level: Run the **pitp port** or **pitp board** command to enable the function at the port level.
 3. VLAN level: Run the **pitp enable** command in VLAN service profile configuration mode.
 4. Service port level: Run the **pitp service-port** command.

----End

Configuring the Internet Access Service (LAN Access, ONU Side)

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 User VLAN ID: 1, 2, 3...	HGWs can send untagged packets or packets with user VLAN tags.

Procedure

Step 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).

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.

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

Configuring the Internet Access Service (ADSL2+ Access, ONU Side)

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.

Background Information

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 2-10](#).

Table 2-10 ADSL2+ profile

Profile Type	Function	Configuration
ADSL2+ line profile	<p>An ADSL2+ line profile provides the following parameters:</p> <ul style="list-style-type: none"> ● ADSL/ADSL2+ working mode ● Channel mode ● Upstream/Downstream line rate ● Upstream/Downstream interleave depth ● Noise margin <p>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.</p>	<p>The system has four default profiles (profile 1, profile 1022, profile 1023, and profile 1024) for activation of ADSL2+ ports in different conditions.</p> <ul style="list-style-type: none"> ● 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. <p>Commands:</p> <ul style="list-style-type: none"> ● To query: display adsl line-profile ● To add: adsl line-profile add or adsl line-profile quickadd
ADSL2+ alarm profile	<p>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.</p>	<p>Commands:</p> <ul style="list-style-type: none"> ● 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.
ADSL2+ line profile	ID: 1024 (default); key parameters: <ul style="list-style-type: none">● 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.

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).

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.

As packets from HGWs contain VPI/VCI information, the PVC needs to be mapped to the user VLAN when a service flow is configured.

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.
- 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

Configuring the Internet Access Service (VDSL2 Access, ONU Side)

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.

Background Information

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 2-11](#).

Table 2-11 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.	<p>The system has one default VDSL2 line template (template 1), which is used for activation of common VDSL2 ports.</p> <ul style="list-style-type: none"> ● To query: display vdsl line-template ● To add: vdsl line-template add or vdsl line-template quickadd

Template Type	Function	Configuration
	<p>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).</p>	<ul style="list-style-type: none"> ● To query: display vdsl line-profile ● To add: vdsl line-profile add or vdsl line-profile quickadd
	<p>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.</p>	<ul style="list-style-type: none"> ● To query: display vdsl channel-template ● To add: vdsl channel-template add or vdsl channel-profile quickadd
VDSL2 alarm template	<p>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.</p>	<p>The system has one default VDSL2 alarm template (template 1).</p> <ul style="list-style-type: none"> ● To query: display vdsl alarm-template ● To add: vdsl alarm-template add or vdsl alarm-template quickadd
	<p>A VDSL2 line alarm profile provides the following parameters for COs and CPEs:</p> <ul style="list-style-type: none"> ● 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 	<ul style="list-style-type: none"> ● To query: display vdsl alarm-profile ● To add: vdsl alarm-profile add or vdsl alarm-profile quickadd
	<p>A VDSL2 channel alarm profile provides the following parameters for COs and CPEs:</p> <ul style="list-style-type: none"> ● Coding violations counts (CVC) ● Corrected blocks counts (CBC) 	<ul style="list-style-type: none"> ● To query: display vdsl channel-alarm-profile ● To add: vdsl channel-alarm-profile add or vdsl channel-alarm-profile quickadd

Data Plan

Table 2-12 provides key information about the Internet access service (VDSL2 access).

Table 2-12 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. <ul style="list-style-type: none"> ● 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.

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).

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 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

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.



WARNING

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 [2.2.5 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	17.10.10.10/24
		Default gateway IP address	17.10.10.1/24
	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 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	
	Ringling current attribute	Default value	

Procedure

Step 1 Log in to and configure the ONU.

Log in to the ONU from the OLT by telnet the management IP address of the ONU. By default, 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 IP address of the Layer 3 interface to 17.10.10.10

```
huawei(config)#interface vlanif 200
huawei(config-if-vlanif200)#ip address 17.10.10.10 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 17.10.10.10 and the MG IP address to 17.10.10.1.

```
huawei(config)#voip
huawei(config-voip)#ip address media 17.10.10.10 17.10.10.1
huawei(config-voip)#ip address signaling 17.10.10.10
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 17.10.10.1 to 200.200.200.0.

```
huawei(config)#ip route-static 200.200.200.0 24 17.10.10.1
```

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 17.10.10.10 mgport
2944 code text transfer udp primary-mgc-ip1 200.200.200.200 primary-mgc-port
2944 mg-media-ip1 17.10.10.10 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)#es1 user
huawei(config-es1-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-es1-user)#mgpstnuser modify 0/3/0 priority cat2
huawei(config-es1-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

Configuring SIP Voice Service (on an 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.



WARNING

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 [2.2.5 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	17.10.10.10/24
		Default gateway IP address	17.10.10.1/24
	SIP interface ID		0
	Signaling port ID		5060
	IP address of the main IMS equipment		200.200.200.200/24

Item		Data
	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 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.

Log in to the ONU from the OLT by telnet the management IP address of the ONU. By default, 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 IP address of the Layer 3 interface to 17.10.10.10

```
huawei(config)#interface vlanif 200
huawei(config-if-vlanif200)#ip address 17.10.10.10 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 17.10.10.10, and the media gateway to 17.10.10.1.

```
huawei(config)#voip
huawei(config-voip)#ip address media 17.10.10.10 17.10.10.1
huawei(config-voip)#ip address signaling 17.10.10.10
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 17.10.10.1 to the network segment 200.200.200.0.

```
huawei(config)#ip route-static 200.200.200.0 24 17.10.10.1
```

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 17.10.10.10 signal-ip
17.10.10.10 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.

```
huawei (config) #save
```

----End

Configuring the IPTV Service (ONU Side)

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.

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.

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
```

- 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

Configuring the Internet Access Service (HGW Side)

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
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 .

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 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.
Encapsulation mode	LLC

- c. Click **OK**.
3. Restart the HGW.
Choose **Management > Device Management** and click **Restarting the Device**.

---End

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.
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 .
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

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.

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.	<p>PPPoE dialup emulation requires a service flow which does not belong to a QinQ VLAN.</p> <p>A user name, password, and authentication mode must be configured on the BRAS for the PPPoE dialup emulation.</p> <p>An ONU supports PPPoE dialup emulation only on one voice port.</p>
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.	<ul style="list-style-type: none"> ● An ONU can emulate the caller or callee in a call to a phone. Therefore, a functioning phone is required in the central equipment room. ● The ONT can emulate the caller or callee simultaneously without off-hook on the port. ● An ONU supports call emulation only on one voice port.
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.
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.

```
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
```

```
-----  
-  
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

2.3.4 FTTB+HGW Networking (HGW Providing the VoIP Service)

In an FTTB+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.

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

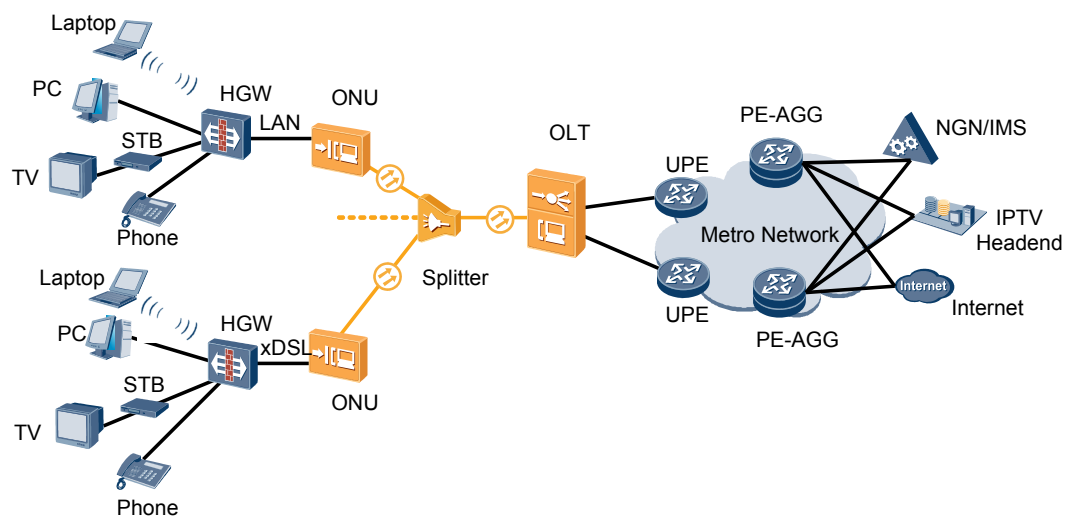
Figure 2-7 shows a GPON FTTB+HGW network. The GPON OLT is deployed at the central office and connects to the MAN using aggregation, and the ONU is deployed in the buildings or street fiber distribution terminals. Access interfaces are deployed on the HGW that connects to the ONU using LAN or xDSL.

- 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: MA5620, MA5626, MA5612, MA5616, MA5652, MA5662, MA5603T. Among these ONUs,

- ONUs with LAN ports include MA5620, MA5626, MA5612, MA5616.
- ONUs with ADSL2+ ports include MA5616, MA5603T.
- ONUs with VDSL2 ports include MA5616, MA5652, MA5662, MA5603T.

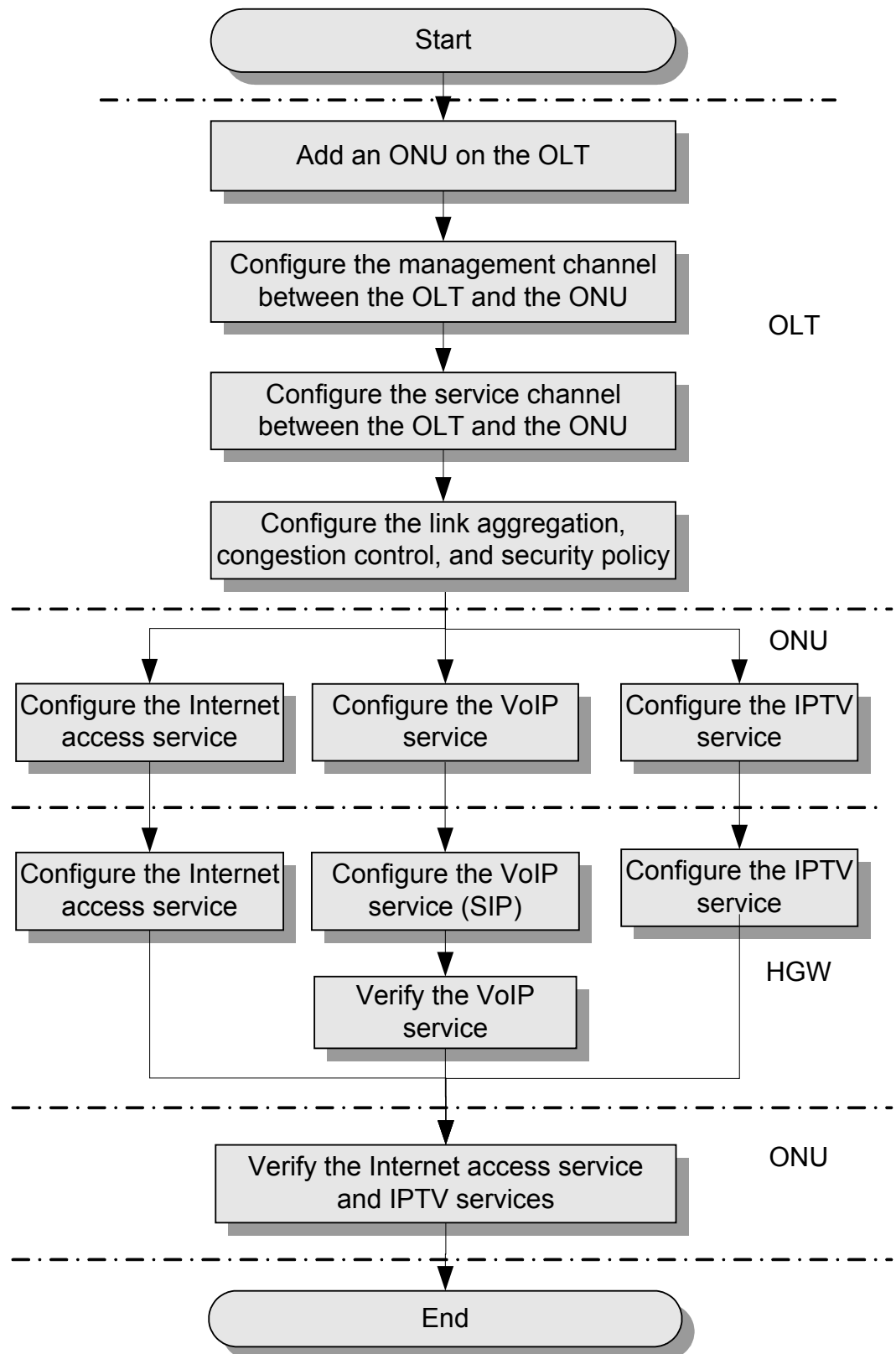
Figure 2-7 GPON FTTB+HGW Networking for the Internet, VoIP, and IPTV Services (HGW Providing the VoIP Service)



Configuration Flow

Figure 2-8 shows the configuration flow for FTTB+HGW networking (HGW providing the VoIP service).

Figure 2-8 Configuration flow for FTTB+HWG networking (HGW providing the VoIP service)



The following table describes each configuration step.

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 from the OLT to 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 from the OLT to the ONU.	<ul style="list-style-type: none"> ● Configure the Internet access service channel. ● Configuring the VoIP service channel. ● Configure the VoD service channel. ● Configuring the multicast service channel. 	In FTTB+HGW networking (HGW providing 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 or each service.
	Configuring Link Aggregation, Congestion Control, and Security Policy		Service reliability is improved by configuring uplink aggregation and priority scheduling policy for upstream queues in global config mode, and service security is improved by configuring security policy in global config mode.
ONU	Configure the Internet access service.	Configuring LAN Internet Access Service (ONU Side)	NOTE In FTTB+HGW networking (HGW providing the VoIP service), the ONU provides LAN, ADSL2+, or VDSL2 Internet access services based on its hardware capabilities. Select one Internet access service based on the ports provided by the ONU during actual configuration.
		Configure the ADSL2+ Internet access service (on the ONU).	

Configured Device	Procedure		Configuration
		<p>Configure the VDSL2 Internet access service (on the ONU).</p>	
	<p>Configure the VoIP service (on the ONU).</p>		<p>In FTTB+HGW networking (HGW providing 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.</p>
	<p>Configure the IPTV services.</p>	<ul style="list-style-type: none"> ● Configure the VoD service. ● Configure the multicast service. 	<p>IPTV services include VoD and multicast services. They differ from each other and need to be configured separately.</p>
HGW	<p>Configure the Internet access service (on the HGW).</p>		<p>HGW products have various models and appearances but their configuration processes are similar. This topic uses home gateways HG239s using LAN upstream transmission and HG527s using ADSL2+ upstream transmission as examples.</p>
	<p>Configure the IPTV services (on the HGW).</p>		-
	<p>Configure the VoIP service (on the HGW).</p>		<p>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.</p>
ONU HGW	<p>Verify Internet access, VoIP, and IPTV services.</p>		<p>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.</p> <p>Voice services on the HGW do not support remote service verification.</p>

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. [Adding an ONU to an OLT](#) is performed.
2. [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.

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 2.2.4 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 2.2.5 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 2.2.6 IPTV Service Data Plan .

Service Type	VLAN Plan	Remarks
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 2.2.6 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.

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 gempport 12 multi-
service user-vlan 1001 tag-transform default 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.

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.

```
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

Configuring Link Aggregation, Congestion Control, and Security Policy

Service reliability is improved by configuring uplink aggregation and priority scheduling policy for upstream queues in global config mode, and service security is improved by configuring security policy in global config mode.

Background Information

In link aggregation, multiple upstream Ethernet ports are aggregated into a group to increase bandwidth and reliability of OLT uplinks. You are advised to configure link aggregation.

In congestion control, queue scheduling is used to put packets from one port into multiple queues and then process the packets based on queue priorities. You are advised to configure congestion control.

Security policy involves system security, user security, and service security, ensuring normal services from different aspects.

 **NOTE**

You are advised to enable the service security feature according to service types. For details, see [2.2.1 Security Design](#).

Procedure

- Configure link 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. The working mode is LACP static aggregation.

```
huawei(config)#link-aggregation 0/19 0-1 ingress workmode lACP-static
```
- Configure queue scheduling.
According to "[2.2.3 QoS Plan](#)", all packets are scheduled in strict priority (SQ) 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 anti-DoS attack.
 1. Run the **security anti-dos enable** command to enable global anti-DoS attack.
 2. Run the **security anti-dos control-packet policy** command to configure the policy of processing protocol packets when a DoS attack occurs.
 3. Run the **security anti-dos control-packet rate** command to configure the threshold of the rate for sending protocol packets to the CPU.
 - Enable anti-ICMP attack.
Run the **security anti-icmpattack enable** command to enable anti-ICMP attack.
 - Enable anti-IP attack.
Run the **security anti-ipattack enable** command to enable anti-IP attack.
- Configure user security.
 - Enables anti-MAC transfer.
Run the **security anti-macduplicate enable** command to enable anti-MAC-duplicate.
 - Enable anti-IP spoofing.
The anti-IP spoofing function can be enabled or disabled at three levels. This anti-IP spoofing function takes effect only when it is enabled at all three levels.
 1. Global level: Run the **security anti-ipspoofing enable** command in global configuration mode.
 2. VLAN level: Run the **security anti-ipspoofing enable** command in VLAN service profile configuration mode.
 3. Service port level: Run the **security anti-ipspoofing service-port serviceport-id enable** command.
- Configure service security.
 - Enable DHCP option 82, which is used in DHCP dialup as recommended.
The DHCP option 82 function can be enabled or disabled at four levels. The DHCP option 82 function takes effect only when it is enabled at all four levels.
 1. Global level: Run the **dhcp option82 enable** command in global configuration mode.

2. Port level: Run the **dhcp option82 port** or **dhcp option82 board** command to enable the function at the port level.
 3. VLAN level: Run the **dhcp option82 enable** command in VLAN service profile configuration mode.
 4. Service port level: Run the **dhcp option82 service-port** command.
- Enable PITP, which is used in PPPoE dialup as recommended.

The PITP function can be enabled or disabled at four levels. The PITP function takes effect only when it is enabled at all four levels.

1. Global level: Run the **pitp enable pmode** command in global configuration mode.
2. Port level: Run the **pitp port** or **pitp board** command to enable the function at the port level.
3. VLAN level: Run the **pitp enable** command in VLAN service profile configuration mode.
4. Service port level: Run the **pitp service-port** command.

---End

Configuring the Internet Access Service (LAN Access, ONU Side)

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 User VLAN ID: 1, 2, 3...	HGWs can send untagged packets or packets with user VLAN tags.

Procedure

Step 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).

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.

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

Configuring the Internet Access Service (ADSL2+ Access, ONU Side)

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.

Background Information

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 2-13](#).

Table 2-13 ADSL2+ profile

Profile Type	Function	Configuration
ADSL2+ line profile	<p>An ADSL2+ line profile provides the following parameters:</p> <ul style="list-style-type: none"> ● ADSL/ADSL2+ working mode ● Channel mode ● Upstream/Downstream line rate ● Upstream/Downstream interleave depth ● Noise margin <p>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.</p>	<p>The system has four default profiles (profile 1, profile 1022, profile 1023, and profile 1024) for activation of ADSL2+ ports in different conditions.</p> <ul style="list-style-type: none"> ● 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. <p>Commands:</p> <ul style="list-style-type: none"> ● To query: display adsl line-profile ● To add: adsl line-profile add or adsl line-profile quickadd
ADSL2+ alarm profile	<p>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.</p>	<p>Commands:</p> <ul style="list-style-type: none"> ● 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	<p>ID: 8</p> <p>CIR: 4 Mbit/s</p> <p>VLAN priority: 0</p> <p>Downstream priority policy: local-setting</p>	A traffic profile implements rate-limiting.
VPI/VCI of ADSL2+ users	<p>VPI: 0</p> <p>VCI: 35</p>	Internet service providers (ISPs) provide VPI/VCI information.

Item	Data	Remarks
ADSL2+ line profile	ID: 1024 (default); key parameters: <ul style="list-style-type: none">● 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.

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).

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.

As packets from HGWs contain VPI/VCI information, the PVC needs to be mapped to the user VLAN when a service flow is configured.

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.

- 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

Configuring the Internet Access Service (VDSL2 Access, ONU Side)

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.

Background Information

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 2-14](#).

Table 2-14 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.	<p>The system has one default VDSL2 line template (template 1), which is used for activation of common VDSL2 ports.</p> <ul style="list-style-type: none"> ● 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).	<ul style="list-style-type: none"> ● To query: display vdsl line-profile ● To add: vdsl line-profile add or vdsl line-profile quickadd

Template Type	Function	Configuration
	<p>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.</p>	<ul style="list-style-type: none"> ● To query: display vdsl channel-template ● To add: vdsl channel-template add or vdsl channel-profile quickadd
VDSL2 alarm template	<p>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.</p>	<p>The system has one default VDSL2 alarm template (template 1).</p> <ul style="list-style-type: none"> ● To query: display vdsl alarm-template ● To add: vdsl alarm-template add or vdsl alarm-template quickadd
	<p>A VDSL2 line alarm profile provides the following parameters for COs and CPEs:</p> <ul style="list-style-type: none"> ● 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 	<ul style="list-style-type: none"> ● To query: display vdsl alarm-profile ● To add: vdsl alarm-profile add or vdsl alarm-profile quickadd
	<p>A VDSL2 channel alarm profile provides the following parameters for COs and CPEs:</p> <ul style="list-style-type: none"> ● Coding violations counts (CVC) ● Corrected blocks counts (CBC) 	<ul style="list-style-type: none"> ● To query: display vdsl channel-alarm-profile ● To add: vdsl channel-alarm-profile add or vdsl channel-alarm-profile quickadd

Data Plan

Table 2-15 provides key information about the Internet access service (VDSL2 access).

Table 2-15 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. <ul style="list-style-type: none"> ● 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.

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).

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 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

Configuring the Voice Service 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.
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.

Item	Data	Remarks
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:

```
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

Configuring the IPTV Service (ONU Side)

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.
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.

Item	Data	Remarks
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.

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
```

- 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

Configuring the Internet Access Service (HGW Side)

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
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.
Encapsulation mode	LLC
 - c. Click **OK**.
 3. Restart the HGW.
Choose **Management > Device Management** and click **Restarting the Device**.

----End

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.
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 .
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

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 uses ADSL2+ 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
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 **Application > 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:

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

Parameter	Value
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	-

- Restart the HGW.

Choose **Management > Device Management** and click **Restarting the Device**.

----End

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.	<ul style="list-style-type: none"> ● 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 call emulation.

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
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:

```
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 [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

3 Configuring the FTTO Service

About This Chapter

Through the "OLT+SBU" network, the fiber to the office (FTTO) solution is provided for enterprise users.

[3.1 Configuring the TDM PBX Access Service \(SDH-based\)](#)

The ONU provides eight E1 ports for connecting to the enterprise TDM PBX, and the OLT transmits signals of the TDM PBX upstream to the SDH network. The ONUs support this service are MA5612 and MA5628.

[3.2 Configuring the Enterprise Router Access Service](#)

The ONU provides FE/GE ports for connecting to the enterprise router or Layer 3 switch, and the OLT transmits signals of the router or switch upstream to the IP network. The ONUs support this service are MA5628.

[3.3 Configuring the IP PBX Access Service](#)

The ONU provides GE/FE ports for connecting to the enterprise IP PBX, and the OLT transmits signals of the IP PBX upstream to the PSN network. The ONUs support this service are MA5628.

[3.4 Configuring the POTS Access Service of the Enterprise](#)

The ASNB board of the ONU provides a 16-channel POTS port for connecting to the analog phone sets of the enterprise, implementing the VoIP service. The ONUs support this service is MA5628.

3.1 Configuring the TDM PBX Access Service (SDH-based)

The ONU provides eight E1 ports for connecting to the enterprise TDM PBX, and the OLT transmits signals of the TDM PBX upstream to the SDH network. The ONUs support this service are MA5612 and MA5628.

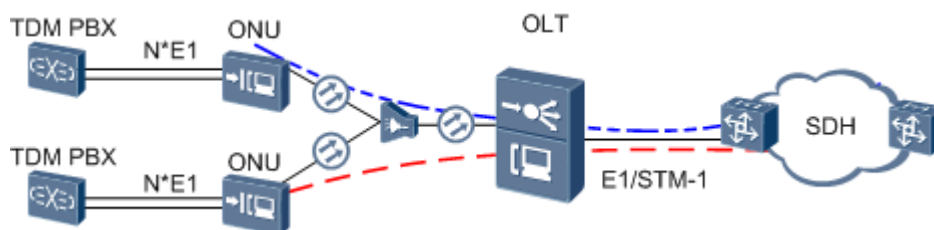
Service Requirements

- The E1 port of the ONU is connected to the enterprise TDM PBX.
- Through line emulation, the TDM service data can be transmitted in the GPON network.
- Signals are transmitted upstream to the OLT through GPON, and the OLT transmits the signals upstream to the SDH network.

Background Information

Figure 3-1 shows an example network of the TDM PBX access service (SDH-based). The ONU provides the PBX access, and the OLT transmits signals upstream to the SDH network through the E1 or STM-1 port.

Figure 3-1 Example network of the TDM PBX access service (SDH-based)



Procedure

In the network, the ONU accesses the TDM PBX in TDM E1 mode and accesses the OLT in native TDM mode. The OLT is upstream connected to the SDH network in E1 or STM-1 mode. The specific data plan and configuration process are the same as those described in [Configuring the Native TDM Base Station Access Service \(SDH-based, MA5612/MA5628\)](#). For details, see [4.3 Configuring the Native TDM Base station access Service \(SDH-based, MA5628\)](#).

3.2 Configuring the Enterprise Router Access Service

The ONU provides FE/GE ports for connecting to the enterprise router or Layer 3 switch, and the OLT transmits signals of the router or switch upstream to the IP network. The ONUs support this service are MA5628.

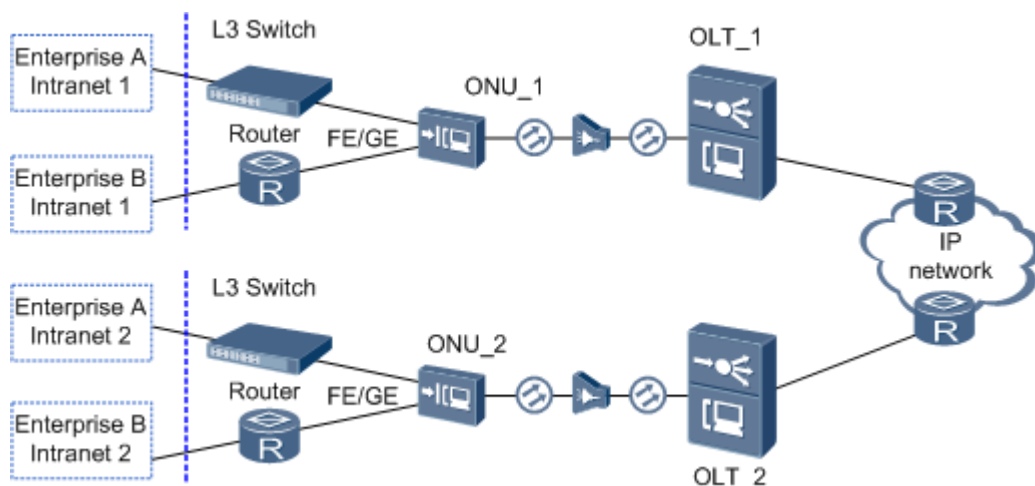
Service Requirements

Provide a transparent and safe data channel for enterprise private networks that are located in different places, so that the service data and BPDUs between enterprise private networks can be transparently transmitted in the public network.

Figure 3-2 shows an example network of the enterprise router access service.

The FE/GE port of the ONU is connected to the enterprise router or Layer 3 switch. Configure the QinQ VLAN encapsulation mode on both ONU_1 and ONU_2 so that data can be transparently transmitted in the GPON network. Signals are transmitted upstream to the OLT through GPON, and then the OLT transmits the signals upstream to the IP network.

Figure 3-2 Example network of the enterprise router access service



Data Plan

Table 3-1 provides the data plan for the OLT, and **Table 3-2** provides the data plan for the ONU.

Table 3-1 Data plan for configuring the enterprise router access service-OLT side

Item	Data
VLAN	Inband management VLAN: smart VLAN 8 SVLAN: smart VLAN 2000 with the attribute QinQ
IP address	Inband management IP address: 192.168.50.1/24
GPON service board	Port: 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 and 1 T-CONT ID: 5
ONU management mode	SNMP

Table 3-2 Data plan for configuring the enterprise router access service-ONU side

Item	Data
VLAN	Inband management VLAN: smart VLAN 8, adding GPON upstream port 0/0/0 to this VLAN SVLAN: smart VLAN 2000 with the attribute QinQ, adding GPON upstream port 0/0/0 to the VLAN Private VLANs of enterprise A and enterprise B: VLAN 50 and VLAN 60
IP address	Inband management IP address: 192.168.50.2/24

Procedure

- **Configure the OLT.**

 **NOTE**

OLT_1 and OLT_2 have the same configuration.

1. Create an SVLAN and add an upstream port to it.

Create smart VLAN 2000 and add upstream port 0/19/0 to it.

```
huawei(config)#vlan 2000 smart
huawei(config)#vlan attrib 2000 q-in-q
huawei(config)#port vlan 2000 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, upstream link aggregation can be configured. For details, see [Configuring Upstream Link Aggregation](#).

3. Configure GPON ONU profiles.

GPON ONU profiles include the DBA profile, line 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.
- 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 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 MDU 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.

```
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 and GEM port 1 for transmitting ETH 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.

 **NOTE**

- a. 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.
- b. 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
```

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, and map the service port of SVLAN 2000 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 2000
```

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-lineprofile-id
10
```

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
//The rest of the response information is omitted.
huawei (config-if-gpon-0/3) #ont confirm 1 ontid 1 sn-auth
48575443E6D8B541 snmp ont-lineprofile-id
10
```

NOTE

If multiple ONUs of the same type are connected to a port and the same line profile or service profile (for an ONT) 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: **ont confirm 1 all sn-auth snmp ont-lineprofile-id 10**.

- b. (Optional) Bind the alarm profile to the ONU.

The default profile (profile 1) is used.

```
huawei (config-if-gpon-0/3) #ont alarm-profile 1 1 profile-id 1
```

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.
```

If the ONU state fails, the ONU fails to be in the up state, or the ONU does not match, refer to the following suggestions to rectify the fault.

- 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 192.168.50.1/24.

```
huawei (config-if-gpon-0/3) #quit
huawei (config) #vlan 8 smart
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.

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 static ip-address
192.168.50.2 mask 255.255.255.0 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-if-gpon-0/3) #quit
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 service port ID to 1, SVLAN ID to 2000, GEM port ID to 1, and CVLAN ID to 2000. Rate limitation for upstream and downstream packets 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 2000 gpon 0/3/1 ont 1 gemport 1 multi-  
service  
user-vlan 2000 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. The priority of the TDM emulation service is 6, adopting the PQ scheduling.

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
```

● **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.

ONU_1 and ONU_2 have the same configuration.

1. Create an SVLAN and add an upstream port to it.

Configure the SVLAN ID to 2000, type to smart, attribute to QinQ, and upstream GPON port to 0/0/0.

```
huawei(config)#vlan 2000 smart  
huawei(config)#vlan attrib 2000 q-in-q  
huawei(config)#port vlan 2000 0/0 0
```

2. (Optional) Enable transparent transmission of BPDUs, and bind VLAN service profile 1 to the SVLAN.

```
huawei(config)#vlan service-profile profile-id 1  
huawei(config-vlan-srvprof-1)#bpd tunnel enable  
Info: Please use the commit command to make modifications take effect  
huawei(config-vlan-srvprof-1)#commit  
huawei(config-vlan-srvprof-1)#quit  
huawei(config)#vlan bind service-profile 2000 profile-id 1
```

3. Create a service port.

Create service ports for VLAN 2000 with the QinQ attribute. The outer VLAN ID is 2000. The router or Layer 3 switch of enterprise A is connected to GE port 0/4/0 of the ONU, and the Intranet packets of enterprise A contain VLAN tag 50; the router or Layer 3 switch of enterprise B is connected to GE port 0/4/1 of the ONU, and the Intranet packets of enterprise B contain VLAN tag 60.

```
huawei(config)#service-port vlan 2000 eth 0/4/0 multi-service user-vlan 50
rx-cttr 6 tx-cttr 6
huawei(config)#service-port vlan 2000 eth 0/4/1 multi-service user-vlan 60
rx-cttr 6 tx-cttr 6
```

4. Save the data.

```
huawei(config)#save
```

---End

Result

The private networks distributed in two places can communicate with each other and various services can be provided between these private networks.

Configuration File

Configure the OLT.

```
vlan 2000 smart
vlan attrib 2000 q-in-q
port vlan 2000 0/19 0
vlan 8 smart
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
mapping-mode vlan
gem mapping 0 0 vlan 8
gem mapping 1 1 vlan 2000
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
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 gempport 0 multi-service
user-vlan 8 rx-cttr 6 tx-cttr 6
service-port 1 vlan 2000 gpon 0/3/1 ont 1 gempport 1 multi-service
user-vlan 2000 rx-cttr 6 tx-cttr 6
queue-scheduler wr 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 2000 smart
vlan attrib 2000 q-in-q
port vlan 2000 0/0 0
vlan service-profile profile-id 1
bpdu tunnel enable
commit
quit
vlan bind service-profile 2000 profile-id 1
```

```
service-port vlan 2000 eth 0/4/0 multi-service user-vlan 50 rx-cttr 6 tx-cttr 6
service-port vlan 2000 eth 0/4/1 multi-service user-vlan 60 rx-cttr 6 tx-cttr 6
save
```

3.3 Configuring the IP PBX Access Service

The ONU provides GE/FE ports for connecting to the enterprise IP PBX, and the OLT transmits signals of the IP PBX upstream to the PSN network. The ONUs support this service are MA5628.

Service Requirements

- The FE/GE port of the ONU is connected to the enterprise IP PBX.
- Data can be transparently transmitted in the GPON network.
- Signals are transmitted upstream to the OLT through GPON, and the OLT transmits the signals upstream to the IP.
- L2 VPN adopts the QinQ VLAN encapsulation mode.

Background Information

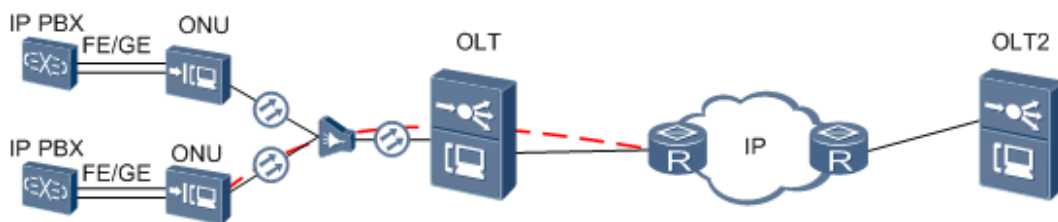
IP PBX is an IP network-based company telephone system. It can integrate voice communication into the data network of the company, setting up an integrated voice and data network that can connect all offices and employees distributed all over the world. For example, the SoftCo series IP voice integrated switch of Huawei can function as a mini NGN system and IP-PBX.

The IP PBX access service is classified into the following scenarios:

- The ONU provides the IP PBX access, and the OLT transmits data transparently to the IP network in the QinQ VLAN mode.

Figure 3-3 shows an example network of the IP PBX access service.

Figure 3-3 Example network of the IP PBX access service



Procedure

- The ONU provides the IP PBX access, and the OLT transmits data transparently to the IP network in the QinQ VLAN mode.

For details about the configuration, see [3.2 Configuring the Enterprise Router Access Service](#).

----End

3.4 Configuring the POTS Access Service of the Enterprise

The ASNB board of the ONU provides a 16-channel POTS port for connecting to the analog phone sets of the enterprise, implementing the VoIP service. The ONUs support this service is MA5628.

Service Requirements

- The enterprise directly uses the existing phone sets for the voice service and no additional investment is required.
- The voice data is carried over the IP network, which reduces the communication costs of the enterprise to a great extent without compromising the communication quality.
- The extensions can call each other using the original internal extension numbers.
- The DBA mode of the VoIP service is assured bandwidth + maximum bandwidth, and no rate limitation is performed on the upstream and downstream traffic.
- The polarity-reversal accounting is adopted.

Prerequisite

- If H.248 is used as the voice protocol, the MGC interface data and the PSTN user data corresponding to the MG interface must be configured on the MGC.
- If SIP is used as the voice protocol, the SIP interface data and the PSTN user data corresponding to the SIP interface must be configured on the IMS.

Background Information

The ONU supports voice protocols H.248 and SIP, but only one is used at a time. You can run the **display protocol support** command to query the currently used voice protocol of the system. To switch between the two voice protocols, ensure that the MG is deleted and run the **protocol support** command. After the configuration is complete, save the configuration and restart the system to make the configured protocol take effect.

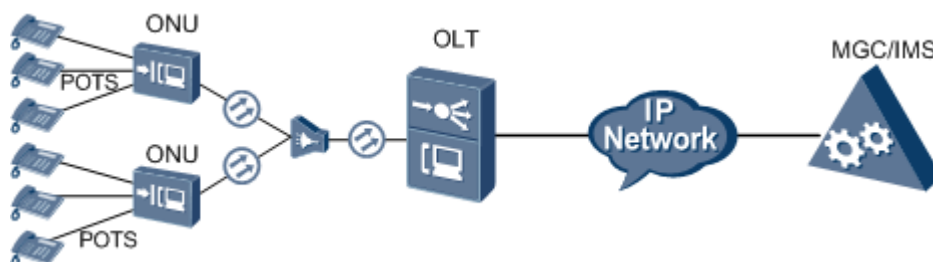


WARNING

This operation interrupts the ongoing services carried on the currently used MG interface. Hence, exercise caution when performing this operation.

Figure 3-4 shows an example network of the POTS access service. The ONU is connected to 16 analog phone sets through the POTS port. After the digital conversion of the voice signals (forming IP packets), the ONU encapsulates them into GEM frames and transmits the GEM frames upstream to the OLT through the GPON. The OLT decapsulates the GEM frames, recovers the IP packets, and forwards them to the MGC on the other side of the IP network. For the ONU, the OLT transparently transmits the voice service.

Figure 3-4 Example network of the POTS access service of the enterprise



Procedure

Step 1 Configure the OLT:

1. Create an SVLAN and add an upstream port to it.

Create smart SVLAN 200 with the attributed common and add upstream port 0/19/0 to VLAN 200.

```
huawei(config)#vlan 200 smart
huawei(config)#port vlan 200 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, upstream link aggregation can be configured. For details, see [Configuring Upstream Link Aggregation](#).

3. Configure the GPON ONU profiles.

GPON ONU profiles include the DBA profile, line 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.
- 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 traffic profiles existing in the system. If the traffic profiles existing in the system do not meet the requirements, you need to run the **dba-profile add** command to add a traffic profile.

Configure the DBA profile name to VOIP, type to Type3, assured bandwidth to 15M bit/s, and maximal bandwidth to 30M bit/s.

```
huawei(config)#dba-profile add profile-name VOIP type3 assure 15360 max 30720
```

- b. Add an ONU line profile.

Add GPON MDU line profile 10 and bind T-CONT 5 to the DBA profile named VOIP. 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 VOIP
```

Add GEM port 0 for transmitting management traffic streams and GEM port 1 for transmitting ETH 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.

 **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
```

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, and map the service port of SVLAN 200 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 200
```

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-
lineprofile-id
10
```

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
//The rest of the response information is omitted.
huawei(config-if-gpon-0/3)#ont confirm 1 ontid 1 sn-auth 48575443E6D8B541
snmp ont-lineprofile-id
10
```

NOTE

If multiple ONUs of the same type are connected to a port and the same line profile or service profile (for an ONT) 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: **ont confirm 1 all sn-auth snmp ont-lineprofile-id 10**.

- b. (Optional) Bind the alarm profile to the ONU.

The default profile (profile 1) is used.

```
huawei(config-if-gpon-0/3)#ont alarm-profile 1 1 profile-id 1
```

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.
```

If the ONU state fails, the ONU fails to be in the up state, or the ONU does not match, refer to the following suggestions to rectify the fault.

- 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 192.168.50.1/24.

```
huawei (config-if-gpon-0/3) #quit
huawei (config) #vlan 8 smart
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.

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 static ip-address
192.168.50.2 mask 255.255.255.0 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-if-gpon-0/3) #quit
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 service port ID to 1, SVLAN ID to 200, GEM port ID to 1, and CVLAN ID to 200. Rate limitation for upstream and downstream packets 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 200 gpon 0/3/1 ont 1 gemport 1 multi-
service
user-vlan 200 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. The priority of the TDM emulation service is 6, adopting the PQ scheduling.

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. Create an SVLAN and add an upstream port to it.

The VLAN ID must be consistent with the CVLAN of the OLT.

Create smart VLAN 200 and add upstream port 0/0/0 to it.

```
huawei(config)#vlan 200 smart
huawei(config)#port vlan 200 0/0/0
```

2. Configure the upstream port of the media stream and the signaling stream.

Create VLAN 200 and add upstream port 0/0/0 to the VLAN. Configure the IP address of the VLAN L3 interface to 17.10.10.10 and subnet mask to 255.255.255.0.

```
huawei(config)#interface vlanif 200
huawei(config-if-vlanif200)#ip address 17.10.10.10 24
huawei(config-if-vlanif200)#quit
```

3. Configure the media and signaling IP address pools.

You can configure the attributes of the SIP 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.

Configure both the media IP address and the signaling IP address to 17.10.10.10, and the media gateway to 17.10.10.1.

```
huawei(config)#voip
huawei(config-voip)#ip address media 17.10.10.10 17.10.10.1
huawei(config-voip)#ip address signaling 17.10.10.10
huawei(config-voip)#quit
```

4. Configure the static route.

Because the IP address of the VLAN interface and the IP address of the IMS are in different network segments, you should configure a route for the network segment from gateway 17.10.10.1 to 200.200.200.0.

```
huawei(config)#ip route-static 200.200.200.0 24 17.10.10.1
```

5. Add an SIP interface.

```
huawei(config)#interface sip 0  
Are you sure to add SIP interface?(y/n) [n]:y
```

6. Configure the basic attributes of the SIP interface.

- Signaling IP address: 17.10.10.10
- Coding mode: text
- Signaling port ID: 5060
- Transfer mode: UDP
- IP address of the primary IMS: 200.200.200.200
- Signaling port ID of the primary IMS: 5060
- Media IP address 1: 17.10.10.10
- Homing domain name of SIP interface: huawei
- SIP profile ID: 1

```
huawei(config-if-sip-0)#if-sip attribute basic media-ip 17.10.10.10  
signal-ip 17.10.10.10 signal-port 5060 transfer udp primary-proxy-ip1  
200.200.200.200 primary-proxy-port 5060 home-domain huawei sipprofile-index  
1
```

7. (Optional) Configure the optional attributes of the SIP interface.

You can configure the optional attributes such as the domain name, description, register server uniform resource identifier (URI), phone context and conference factory URI by running command **if-sip attribute optional**. No configuration here.

8. 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
```

9. Configure the PSTN user data.

Configure the telephone number of the user on port 0/3/1 to 0/3/16 in batches, telephone number of the user from 83110001 to 83110016.

 **NOTE**

- To configure the PSTN data of a single user, run the **sippstnuser add** command.
- To configure the PSTN data of multiple users in batches, run the **sippstnuser batadd** command.

```
huawei(config)#esl user  
huawei(config-esl-user)#sippstnuser batadd 0/3/1 0/3/16 0 telno 83110001
```

10. Change the call priority of the PSTN user.

Configure the call priority of the user on port 0/3/1 to Cat2 and the users of 0/3/2 to 0/3/16 to Cat3 (Default).

```
huawei(config-esl-user)#sippstnuser attribute set 0/3/1 priority cat2  
huawei(config-esl-user)#quit
```

11. Modify the attributes of all the PSTN ports so that the PSTN ports support the polarity reversal.

Modify the attributes of the PSTN port 0/3/1 to 0/3/16 so that the PSTN ports supports the polarity reversal.

```
huawei(config)#pstnport  
huawei(config-pstnport)#pstnport attribute batset 0/3/1 0/3/16 reverse-pole-
```

```
pulse enable
huawei(config-pstnport)#quit
```

12. Save the data.

```
huawei(config)#save
```

----End

Result

After the configuration is completed, users can make calls between two phones.

- 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 ringback 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

Configure the OLT.

```
vlan 200 smart
port vlan 200 0/19 0
dba-profile add profile-name VoIP type3 assure 15360 max 30720
ont-lineprofile gpon profile-id 10
tcont 2 dba-profile-name VoIP
gem add 0 eth tcont 5 priority-queue 3 cascade on
gem add 1 eth tcont 5 priority-queue 3 cascade on
mapping-mode vlan
gem mapping 0 0 vlan 8
gem mapping 1 1 vlan 200
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
ont alarm-profile 1 1 profile-id 1
quit
vlan 8 smart
interface vlanif 8
ip address 192.168.50.1 24
quit
interface gpon 0/3
ont ipconfig 1 1 static ip-address 192.168.50.2 mask 255.255.255.0 vlan 8
quit
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 200 gpon 0/3/1 ont 1 gemport 1 multi-service
  user-vlan 200 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 200 smart
port vlan 200 0/0 0
interface vlanif 200
ip address 17.10.10.10 24
quit
voip
ip address media 17.10.10.10 17.10.10.1
```

```
ip address signaling 17.10.10.10
quit
ip route-static 200.200.200.0 24 17.10.10.1
interface sip 0
if-sip attribute basic media-ip 17.10.10.10 signal-ip 17.10.10.10 signal-port 5060
transfer udp primary-proxy-ip1 200.200.200.200
    primary-proxy-port 5060 home-domain huawei sipprofile-index 1
reset
quit
esl user
sippstnuser batadd 0/3/1 0/3/16 0 telno 83110001
sippstnuser attribute set 0/3/1 priority cat2
quit
pstnport
pstnport attribute batset 0/3/1 0/3/16 reverse-pole-pulse enable
quit
save
```

4 Configuring the Base station access Service

About This Chapter

In the base station access network, the ONU, functioning as a cell backhaul unit (CBU), is connected to the 2G or 3G base station in various modes. The OLT connects the ONU to the base station controller (BSC) or radio network controller (RNC), and transmits signals to the upper-layer network. In this way, the ONU implements the base station access network application over the 2G or 3G network.

Context

NOTE

The PTN refer to the CX 600 unless otherwise specified.

[4.1 Configuring Base station access Clock Synchronization](#)

This topic describes the concept and principle of clock synchronization in base station access network, clock synchronization solutions supported by devices, and configuration differences.

[4.2 Configuring Base Station Access Network Protection](#)

In the base station access application, Type B, Type C single homing or Type C dual homing (Applies only to the the QinQ base station access) protection is recommended between the ONU and the OLT, and link aggregation protection or STM-1 protection are recommended for upstream links.

[4.3 Configuring the Native TDM Base station access Service \(SDH-based, MA5628\)](#)

The ONU is connected to the 2G or 3G base station in the TDM E1 mode and the OLT in the Native TDM mode. The OLT is connected upstream to the SDH network through the E1 or STM-1 port, carrying the traditional circuit switched service over the GPON network.

[4.4 Configuring the Native TDM Base station access Service \(SDH-based, OT928G\)](#)

The ONU is connected to the 2G or 3G base station in the TDM E1 mode and the OLT in the Native TDM mode. The OLT is connected upstream to the SDH network through the E1 or STM-1 port, carrying the traditional circuit switched service over the GPON network.

[4.5 Configuring the QinQ Private Line Base station access Service for the OLT](#)

The ONU is connected to the IP-based station through the FE/GE port and the OLT transmits the QinQ private line service to the MAN device, implementing the base station access service. The ONUs support this service are MA5628.

4.1 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.

4.1.1 Overview of Base station access Clock Synchronization

This topic describes the clock synchronization concept, clock 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.

Clock Synchronization

In a narrow sense, clock synchronization refers to frequency synchronization and time synchronization refers to frequency and phase synchronization. In a broad sense, clock synchronization includes frequency synchronization and phase synchronization. Unless otherwise stated, clock synchronization refers to frequency synchronization and phase synchronization.

Clock synchronization means that all digital devices running in the communications network trace the same average rate so that the written clock rate and the read clock rate are maintained within the same error range, ensuring that data is correctly transmitted and processed.

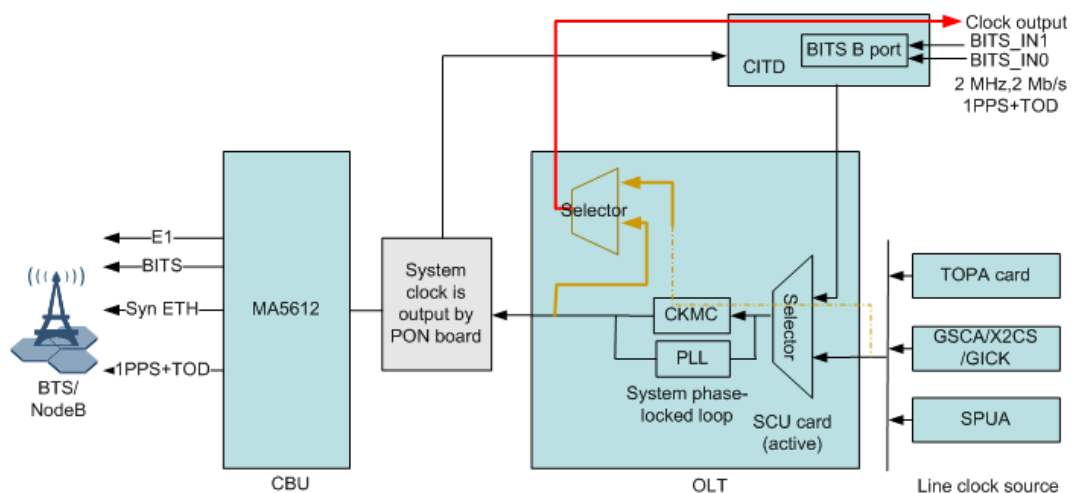
In a traditional communications network architecture, the TDM service of the fixed network is mainly voice service. Cumulative inconsistency between the clocks at both ends of the bearer network over a long time causes frame slip. On a communications network, the wireless application has the most rigorous requirements on the clock frequency. The frequencies of different base stations must be synchronized within a specified precision. Otherwise, re-sync occurs during the base station switching.

The purpose of clock 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.

Clock Synchronization Solution

Figure 4-1 shows a clock synchronization solution in an FTTM network. The clock 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 4-1 Clock synchronization solution in an base station access network



The figure shows that the OLT can obtain the following clock sources:

- BITS clock source
- E1/STM-1 line clock source
- Synchronous Ethernet line clock
- Internal clock sources are not recommended because they are in free oscillation state and do not have advantages in precision.

Comparison of Clock Synchronization Solution

Table 4-1 shows a clock synchronization solution in an FTMM network.

Table 4-1 Comparison of clock 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: <ul style="list-style-type: none"> ● G.8262 features when CKMC 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)

Synchronization Solution	Usage Scenario	Advantage	Limitation or Hardware Requirements
E1/STM-1 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.	<ol style="list-style-type: none"> 1. Clock precision meets the following requirements: <ul style="list-style-type: none"> ● G.8262 features when CKMC 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. 	<ol style="list-style-type: none"> 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. <p>Boards that support this feature:</p> <ul style="list-style-type: none"> ● 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) or H801TOPA (configured with the H801EH1A daughter board).

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.	<ol style="list-style-type: none"> Clock precision meets the following requirements: <ul style="list-style-type: none"> G.8262 features when CKMC stratum-3 clock units are configured EEC specifications defined in G.8261 when no stratum-3 clock units are configured No requirements on delay, jitter, or pack loss of a PSN network 	<ol style="list-style-type: none"> Ethernet clocks require that MAN PSN networks have the capability of synchronizing Ethernet clocks. Ethernet clocks support only frequency synchronization. <p>Boards that support this feature: H801X2CS, H801GSCA, H801GICK, and H801SPUA</p>

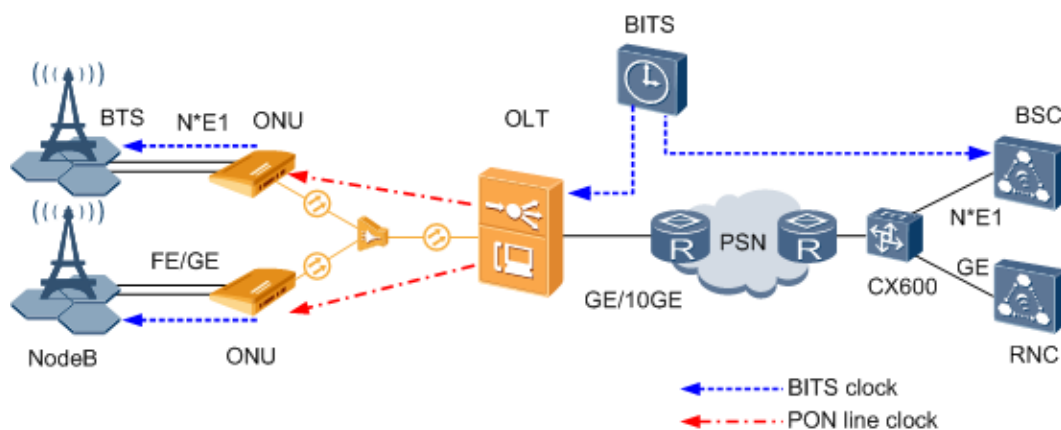
4.1.2 Configuring BITS Clock Synchronization

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 4-2](#), 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 4-2 BITS clock synchronization



Prerequisite

- The clock daughter board CKMC 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.

The clock module automatically judges the types of the specified clock sources (BITS), and sends them according to their priorities to the clock module, serving as clock sources for phase lock.

```
huawei (config) #clock source 0 0/0/0
huawei (config) #clock source 1 0/0/1
```

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.

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 0/0/0
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 FE/GE 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
-----
```

- 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	Config	Type	Source	State	Priority	Output
0	YES	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

Result

After the FTTM service configuration 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.

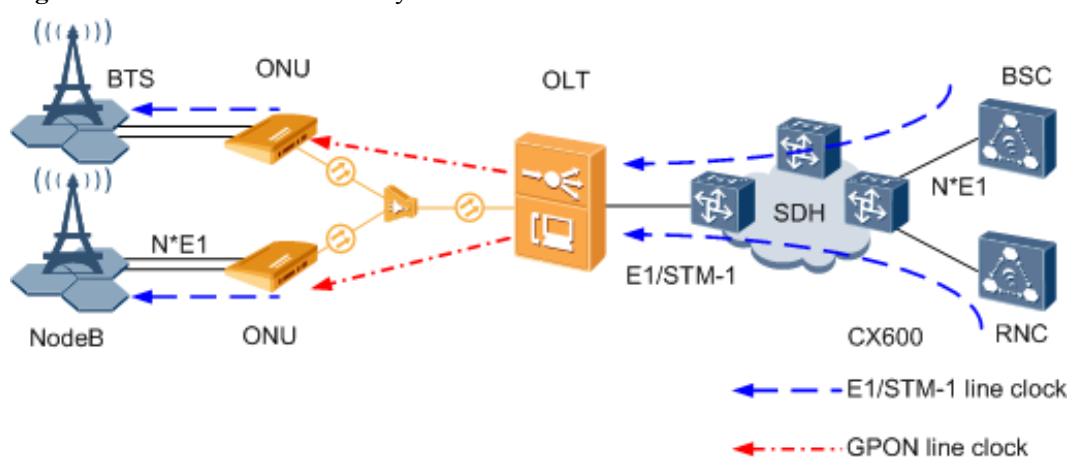
4.1.3 Configuring E1/STM-1 Line Clock Synchronization

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 4-3](#), 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 GPON line clock. After recovering the clock, the ONU transmits the clock to the base station through the E1 line.

Figure 4-3 E1/STM-1 line clock synchronization



Prerequisite

The clock daughter board CKMC of the SCU board must be in position.

Data Plan

Item	Data
TOPA board	Port ID: 0/5/0 Daughter board type: <ul style="list-style-type: none"> 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 GPON service board.
3. The ONU uses the line clock of the GPON 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 sends them according to their priority to the clock module, 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 GPON line clock source as the system clock.

The system clock of the OLT is issued to the ONU through the optical path of the GPON port, implementing the 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 source of the ONU.
- b. Run the **clock priority** command to configure the priority of the clock source.

```
huawei(config)#clock source 0 0/0/0
Clock source set succeeded
```

```
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  Config  Type  Source      State  Priority  Output
-----
0      YES     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

Result

After the FTTM service configuration 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.

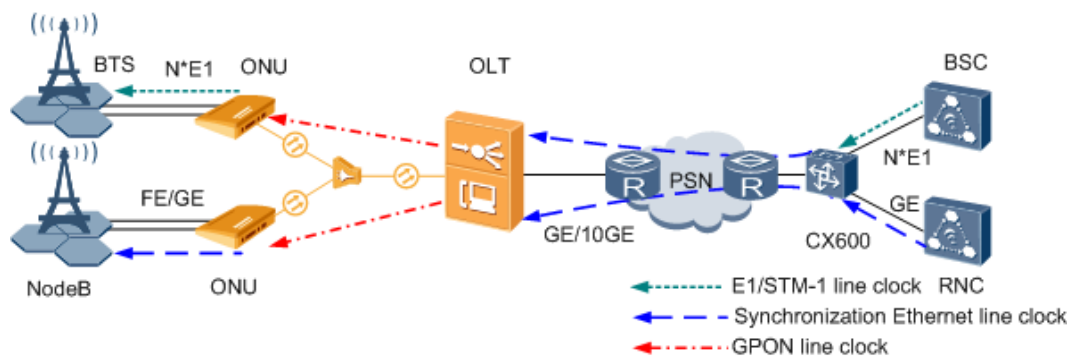
4.1.4 Configuring Ethernet Clock Synchronization

When optical line terminals (OLTs) access a base transceiver station (BTS) that requires only frequency synchronization, such as GSM/WCDMA 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.

Application Context

As shown in **Figure 4-4**, 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 4-4 Ethernet clock synchronization



Prerequisite

- The clock daughter board CKMC of the SCU board must be in position.
- The GIU upstream board must be GICK/GSCA (GE port) or X2CS (10GE port).
- 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	0/4/0

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.
4. The Tx clock of the E1 or FE/GE 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 sends them according to their priorities to the clock module, 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 0/0/0
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 FE/GE 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	Config	Type	Source	State	Priority	Output
0	YES	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

Result

After the FTTM service configuration 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.

4.2 Configuring Base Station Access Network Protection

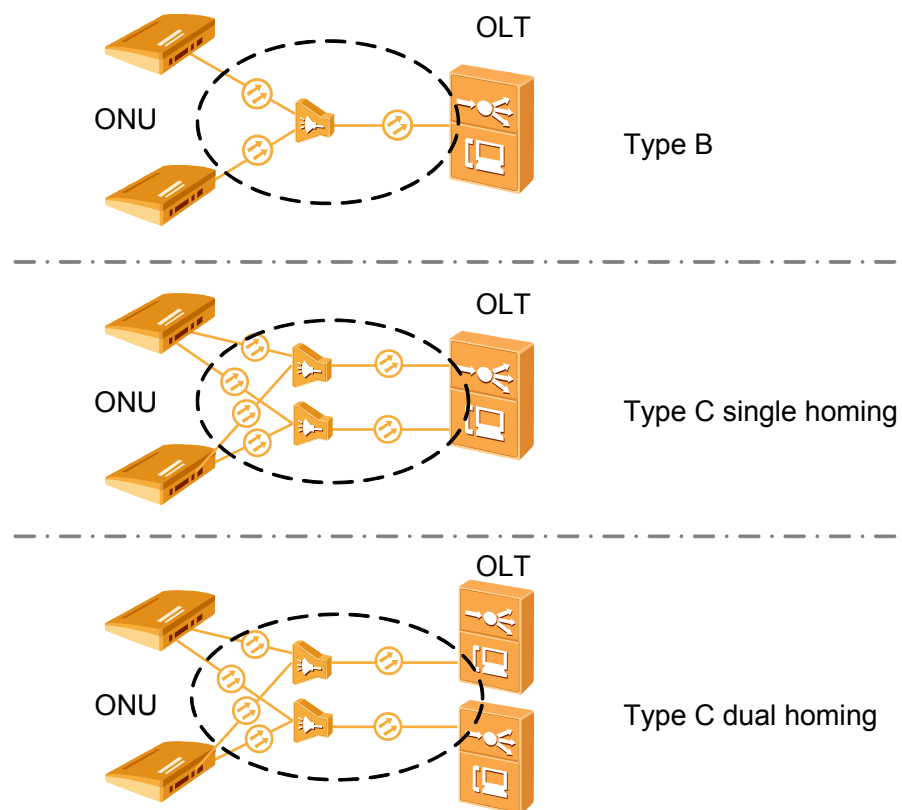
In the base station access application, Type B, Type C single homing or Type C dual homing (Applies only to the the QinQ base station access) protection is recommended between the ONU and the OLT, and link aggregation protection or STM-1 protection are recommended for upstream links.

Background Information

The base station access network can be protected on the device layer or service layer. There are following protection modes:

- Type B, Type C single homing or Type C dual homing protection [Figure 4-5](#) shows the networking differences between them.
 - Type B protection: Two PON ports on the same OLT protect each other. When one of the PON ports fails, the system automatically switches the services to the other PON port. Based on this protection mode, the protection in case of failure of the master port on one OLT is implemented.
 - Type C single homing protection: Type C protection is implemented through the redundancy configuration of the two PON ports on the same OLT, two PON ports on the ONU, backbone optical fiber, optical splitter, and tributary optical fiber. Each item is in a dual configuration.
 - Type C dual homing protection: Type C dual homing protection is implemented through the redundancy configuration of the PON ports on two OLTs, two PON ports on the ONU, backbone optical fiber, optical splitter, and distributed fiber. Each item is in a dual configuration. Different from Type C single homing protection, the ONU is registered with two OLTs.
- STM-1 protect group: Two upstream STM-1 ports can be configured as protect members.
- Link aggregation: The link aggregation group aggregates multiple Ethernet ports as an aggregation group to increase the bandwidth and share the incoming/outgoing load of each member port. At the same time, the ports in an aggregation group back up each other, which increases the link security.

Figure 4-5 Networking differences between Type B, Type C single homing and Type C dual homing protection



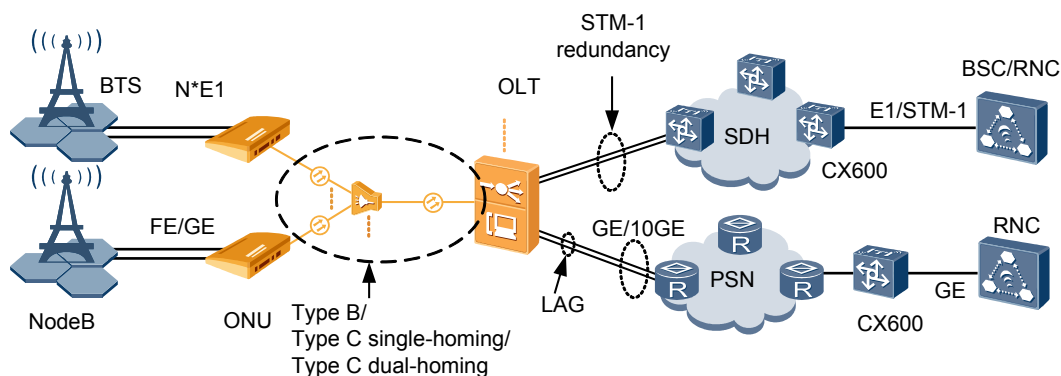
Application Context

As shown in [Figure 4-6](#).

- Type B, Type C single homing and Type C dual homing networking mode can be adopted between the OLT and the ONU for redundancy backup.
- When the OLT transmits services upstream to the SDH network through the STM-1 ports, the STM-1 port protect group can be adopted for redundancy backup.
- When the OLT transmits services upstream to the SDH network through the GE/10GE ports, link aggregation mode between GE/10GE ports can be adopted for redundancy backup.

In actual applications, select the proper protection mode according to the actual network.

Figure 4-6 Base station access network protection



Procedure

- Configure Type B protection.
 1. Run the **protect-group** command to add a protect group.
Pay attention to the following points during the configuration:
 - Configure **protect-target** to **gpon-uni-port**.
 - The working mode of the GPON port protect group must be **timedelay**.
 2. Run the **protect-group member** command to add members to the protect group.
Pay attention to the following points during the configuration:
 - When adding members to the protect group, add a working member, and then add a protection member.
 - The member ports can be ports on different boards, but the board types must be the same.
 3. Run the **protect-group enable** command to enable the protect group.
 4. Run the **display protect-group** command to query the information about the protect group.
- Configure Type C single homing protection.

NOTE

After Type C protection is configured, the configurations of the services that the ONU accesses remain the same as that before the protection is configured. That is, the configuration of services only applies to the active PON ports on the OLT and active upstream PON ports on the ONU.

1. Add an active ONU.
Run the **ont add** command to add ONUs on the active side.
2. Add a standby ONU.
Run the **ont add portid protect-side** command to add a standby ONU on the protection side. Select **protect-side**.
3. Add members to the protect group.
Run the **protect-group member** command to add the ONU registered with the active GPON port of the OLT to the protect group.
4. Add members to the protect group.

Run the **protect-group member** command to add the ONU registered with the standby GPON port of the OLT to the protect group.

 **NOTE**

The value of **ont ontid** must be the same as the specified ONT ID in step 1.

5. Enable the protect group.

Run the **protect-group enable** command to enable the GPON protect group.

- Configure Type C dual homing protection.

 **NOTE**

In the Type C dual homing mode, the ONU registers with two OLTs. Therefore, another two ONUs need to be connected to the two OLTs and the OLTs are configured with protect groups. The following text describes the configurations on the active OLT and standby OLT.

1. Configure the active OLT.

- a. Run the **ont add** command to add an active ONU.
- b. Run the **protect-group** command to create a protect group.

Pay attention to the following points during the configuration:

- Set the **protect-target** to **gpon-uni-port**.
- The working mode of the GPON port protect group must be **dual-parenting**.

- c. Run the **protect-group member** command to add working member to the protect group.

 **NOTE**

After a working member of a dual homing protect group is added, the protect group is enabled automatically.

2. Configure the standby OLT.

- a. Run the **ont add** command to add a standby ONU.

All profiles (such as the line profile and DBA profile) of the active/standby ONUs must be the same.

- b. Run the **protect-group** command to create a protect group.
 - The indexes of the protect groups created on the active and standby OLTs must be the same.
 - Set the **protect-target** to **gpon-uni-port**.
 - The working mode of the GPON port protect group must be **dual-parenting** mode.

- c. Run the **protect-group member** command to add members to the protect group.
- d. Run the **protect-group enable** command to enable the protect group.

- Configure link aggregation.

1. Run the **link-aggregation** command to add a link aggregation group.

Configuration description: When you run the **link-aggregation** command, if **frameid/slotid** is entered twice, inter-board aggregation is configured; if **frameid/slotid** is entered only once, intra-board aggregation is configured.

2. (Optional) Run the **link-aggregation add-member** command to add members to the aggregation group.

Configuration description: This step is optional and is recommended if you need to further increase the bandwidth of an aggregation group or improve the link reliability.

3. Run the **display link-aggregation** command to query the information about the aggregation group.
- Configure an STM-1 upstream port protect group.
 1. Run the **protect-group** add a protect group.
Pay attention to the following points during the configuration:
 - Configure **protect-target** to **stm-nni-port**.
 - The working mode of the STM-1 port protect group can be only **unidirection**.
 2. Run the **protect-group member** command to add members to the protect group.
Pay attention to the following points during the configuration:
 - When adding members to the protect group, add a working member, and then add a protection member.
 - The member ports can be ports on different boards, but the board types must be the same.
 3. Run the **protect-group enable** command to enable the protect group.
 4. Run the **display protect-group** command to query the information about the protect group.

----End

Example

To configure Type B protection for ports 0/3/1 and 0/3/2 on the same GPON board of the OLT, so that when port 0/3/1 is faulty, the system can automatically switch the service to port 0/3/2 to continue service access, do as follows:

```
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
```

To configure Type C single homing protection for the optical link between the OLT and ONU.

- Ports on the same GPON service board are 0/3/1 and 0/3/2.
- The link of port 0/3/1 is on the active side.
- The link of port 0/3/2 is on the protect side.
- The ONU ID is 0.
- ONU adopts SN authentication. The SN is hwhw-10101500 and the management mode is SNMP.
- The ID of the line profile bound with the ONU is 10.

Do as follows:

```
huawei (config) #interface gpon 0/3
huawei (config-if-gpon-0/3) #ont add 0 0 sn-auth hwhw-10101500 snmp ont-lineprofile-
id 10
huawei (config-if-gpon-0/3) #ont add 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 0 role work
huawei (protect-group-1) #protect-group member port 0/3/2 ont 0 role protect
huawei (protect-group-1) #protect-group enable
huawei (protect-group-1) #quit
```

To configure Type C dual homing protection for two OLTs (huawei_A and huawei_B). Specifically,

- huawei_A is the active OLT and huawei_B is the standby OLT.
- The ports on the GPON service board of the two OLTs are both 0/3/1.
- The index of the dual homing protect group is 1.
- The ONU ID is 0.
- ONU adopts SN authentication. The SN is hwhw-10101500 and the management mode is SNMP.
- The ID of the line profile bound with the ONU is 10.

```
Configuration on the active OLT huawei_A:
huawei_A(config)#interface gpon 0/3
huawei_A(config-if-gpon-0/3)#ont add 0 0 sn-auth hwhw-10101500 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 0 role work
Configuration on the standby OLT huawei_B
huawei_B(config)#interface gpon 0/3
huawei_B(config-if-gpon-0/3)#ont add 0 0 sn-auth hwhw-10101500 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 0 role protect
huawei_B(protect-group-1)#protect-group enable
```

Configure link aggregation: The OLT transmits services upstream through the GIU board, upstream ports 0/19/0 and 0/19/1 on the same GIU board are configured as an upstream port aggregation group, packets are distributed to the member ports of the aggregation group according to the source MAC address, and the working mode is the LACP static aggregation mode. To perform these configurations, do as follows:

```
huawei(config)#link-aggregation 0/19 0-1 ingress workmode lacp-static
```

Configure an STM-1 upstream port protect group: Configure STM-1 ports 0/5/0 and 0/5/1 of the TOPA board as a protect group. When the protected port 0/5/0 has a fault or line fault, the system immediately and automatically switches the services from 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
```

4.3 Configuring the Native TDM Base station access Service (SDH-based, MA5628)

The ONU is connected to the 2G or 3G base station in the TDM E1 mode and the OLT in the Native TDM mode. The OLT is connected upstream to the SDH network through the E1 or STM-1 port, carrying the traditional circuit switched service over the GPON network.

Prerequisites

The corresponding hardware requirements must be met:

- OLT adopting the E1 port for upstream transmission: TOPA+NH1A
- OLT adopting the STM-1 port for upstream transmission: TOPA+O2CE
- GPON boards: GPBC and GPBD

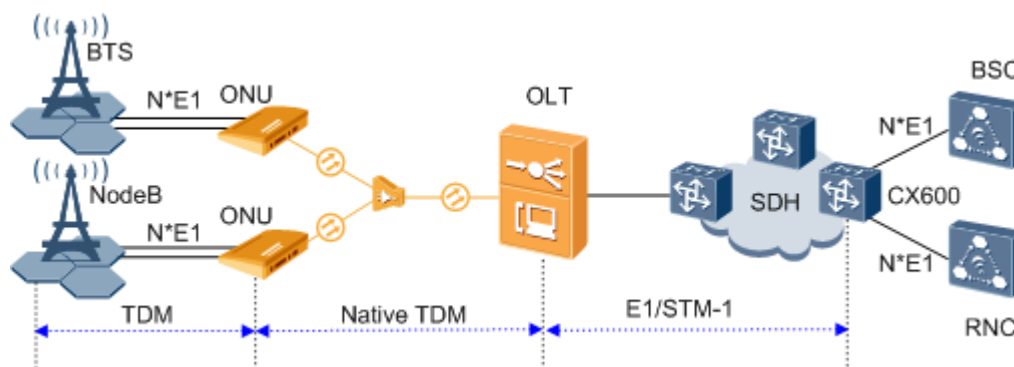
Service Requirements

- The E1 port is used for connecting to the 2G or 3G base station in a unified manner.
- GPON is adopted for bearing the mobile AN in a unified manner to meet mobile carriers' requirements for high bandwidth and high-density coverage of base stations.
- Make full use of existing SDH resources to transmit the TDM service with high quality.

Figure 4-7 shows an example network of the Native TDM base station access service.

The ONU is connected to the 2G or 3G base station through the E1 port to provide the TDM access, and then transmits the service data upstream to the GPON service board of 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) of the TOPA board. In this way, the 2G or 3G base station access service is implemented between the ONU and the OLT in the native TDM mode.

Figure 4-7 Native TDM base station access service



Data Plan

Table 4-2 provides the data plan for the OLT, and Table 4-3 provides the data plan for the ONU.

Table 4-2 Data plan for configuring the Native TDM base station access service-OLT side

Item	Data
VLAN	Inband management VLAN: smart VLAN 8 WARNING When the ONU is connected to the E1 service in native TDM mode, the system always uses VLANs 4000-4007. Hence, these VLANs should not be used in VLAN planning for the OLT or ONU. If these VLANs are used, ONU configuration fails. Consequently, services will be interrupted.
IP address	Inband management IP address: 192.168.50.1/24
GPON service board	Port: 0/3/1 ONU ID: 1 ONU authentication mode: SN ONU SN: 48575443E6D8B541

Item	Data
TOPA service board	Port: 0/5/0 Daughter board type: NH1A (providing E1 ports) or O2CE (providing STM-1 ports) VC12 ID: 2 (for only the STM-1 port)
DBA profile	Profile name: TDM Type: type1 Fixed bandwidth: 32 Mbit/s Dynamic bandwidth allocation mode of GPON ports: minimum bandwidth delay
ONU line profile	<ul style="list-style-type: none"> ● Profile ID: 10 ● GEM port IDs: 0 and 1 ● T-CONT IDs: 1 and 10 ● Bind T-CONT 1 to the DBA profile named TDM ● Bind T-CONT 10 to the DBA profile ID 1
ONU management mode	SNMP

Table 4-3 Data plan for configuring the Native TDM base station access service-ONU side

Item	Data
VLAN	Inband management VLAN: smart VLAN 8, adding GPON upstream port 0/0/0 to this VLAN
IP address	Inband management IP address: 192.168.50.2/24
E1 port	Port: 0/1/0 Working mode of the port: UDT Transmit clock of the port: system

Procedure

- **Configure the OLT.**

1. Configure GPON ONU profiles.

GPON ONU profiles include the DBA profile, line 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.

- 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 DBA profile name to TDM, type to type1, fixed bandwidth to 32 Mbit/s, and enable the bandwidth compensation. Configure the dynamic bandwidth allocation mode of GPON port 0/3/1 to minimum bandwidth delay.

To configure the DBA profile of fixed bandwidth type to bear the TDM services, you must enable the bandwidth compensation function and configure the dynamic bandwidth allocation mode of the GPON port to minimum bandwidth delay.

```
huawei (config) #dba-profile add profile-name TDM type1 fix 32768
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
```

b. Add an ONU line profile.

Add GPON ONU line profile 10, bind T-CONT 10 to default DBA profile named dba-profile_1 and T-CONT 1 to DBA profile named TDM. 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 10 dba-profile-name dba-
profile_1
huawei (config-gpon-lineprofile-10) #tcont 1 dba-profile-name TDM
```

Add GEM port 0 for transmitting management traffic streams and GEM port 1 for transmitting TDM traffic streams. Bind GEM port 0 to T-CONT 10 and GEM port 1 to T-CONT 1. Configure the QoS mode to priority-queue (default) and the queue priority to 0.

 **NOTE**

- a. 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.
- b. 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 10 priority-
queue 0
huawei (config-gpon-lineprofile-10) #gem add 1 tdm tcont 1 priority-
queue 0
```

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, and map the E1 port 1 of the ONU to GEM port 1.

```
huawei (config-gpon-lineprofile-10) #gem mapping 0 0 vlan 8
huawei (config-gpon-lineprofile-10) #gem mapping 1 1 e1 1
```

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.

2. 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.

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
```

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
//The rest of the response information is omitted.
```

```
huawei (config-if-gpon-0/3) #ont confirm 1 ontid 1 sn-auth
48575443E6D8B541 snmp ont-lineprofile-id
10
```

 **NOTE**

If multiple ONUs of the same type are connected to a port and the same line profile or service profile (for an ONT) 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 ONU_0/3/1`.

b. (Optional) Bind the alarm profile to the ONU.

The default profile (profile 1) is used.

```
huawei(config-if-gpon-0/3)#ont alarm-profile 1 1 profile-id 1
```

3. 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.
```

If the ONU state fails, the ONU fails to be in the up state, or the ONU does not match, refer to the following suggestions to rectify the fault.

- 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.

4. 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 192.168.50.1/24.

```
huawei(config-if-gpon-0/3)#quit  
huawei(config)#vlan 8 smart  
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.

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 static ip-address
192.168.50.2 mask 255.255.255.0 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-if-gpon-0/3) #quit
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
```

5. 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.
6. Configure the TDM connection.

Set up a native TDM connection between GEM port 1 and upstream port 0/5/0 of the TPOA board.

- In the case of the E1 upstream port, the configuration is as follows:

```
huawei (config) #tdm-connect connectid 1 tdm 0/5/0 gpon 0/3/1 ontid 1
gemportIndex 1
```

- In the case of the STM-1 upstream port, you must configure the VC12 parameter. VC12 is the virtual container that carries the E1 service. One STM-1 port contains 63 E1 ports. Accordingly, there are 63 VC12 virtual containers. The configuration is as follows:

```
huawei (config) #tdm-connect connectid 1 tdm 0/5/0 vc12 2 gpon 0/3/1
ontid 1 gemportIndex 1
```

7. Configure the system clock and time synchronization.
For details, see [4.1.3 Configuring E1/STM-1 Line Clock Synchronization](#).
8. Configure network protection.
For details, see [4.2 Configuring Base Station Access Network Protection](#).
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. The priority of the TDM emulation service is 6, adopting the PQ scheduling.

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
```

● **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. Configure the system clock synchronization.

For details, see [4.1.3 Configuring E1/STM-1 Line Clock Synchronization](#).

2. Save the data.

```
huawei(config)#save
```

----End

Result

Mobile terminals (mobile phones) near the base station can obtain their network information normally and make calls and send messages to each other normally.

Configuration File

Configure the OLT.

```
vlan 8 smart  
interface vlanif 8  
ip address 192.168.50.1 24  
quit  
dba-profile add profile-name TDM type1 fix 32768 bandwidth_compensate yes  
interface gpon 0/3  
port dba bandwidth-assignment-mode 1 min-loop-delay  
quit  
ont-lineprofile gpon profile-id 10  
tcont 10 dba-profile-name dba-profile_1  
tcont 1 dba-profile-name TDM  
gem add 0 eth tcont 10 priority-queue 0  
gem add 1 tdm tcont 1 priority-queue 0  
gem mapping 0 0 vlan 8  
gem mapping 1 1 e1 1  
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  
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 gempport 0 multi-service  
user-vlan 8 rx-cttr 6 tx-cttr 6  
tdm-connect connectid 1 tdm 0/5/0 gpon 0/3/1 ontid 1 gempportIndex 1 //E1 upstream  
tdm-connect connectid 1 tdm 0/5/0 vc12 2 gpon 0/3/1 ontid 1 gempportIndex 1 //STM-1  
upstream  
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.

```
clock source 0 0/0/0  
clock priority system 0  
interface tdm 0/1  
port 0 udt system
```

```
quit  
save
```

4.4 Configuring the Native TDM Base station access Service (SDH-based, OT928G)

The ONU is connected to the 2G or 3G base station in the TDM E1 mode and the OLT in the Native TDM mode. The OLT is connected upstream to the SDH network through the E1 or STM-1 port, carrying the traditional circuit switched service over the GPON network.

Prerequisites

The corresponding hardware requirements must be met:

- OLT adopting the E1 port for upstream transmission: TOPA + NH1A
- OLT adopting the STM-1 port for upstream transmission: TOPA + O2CE
- GPON boards: GPBC and GPBD

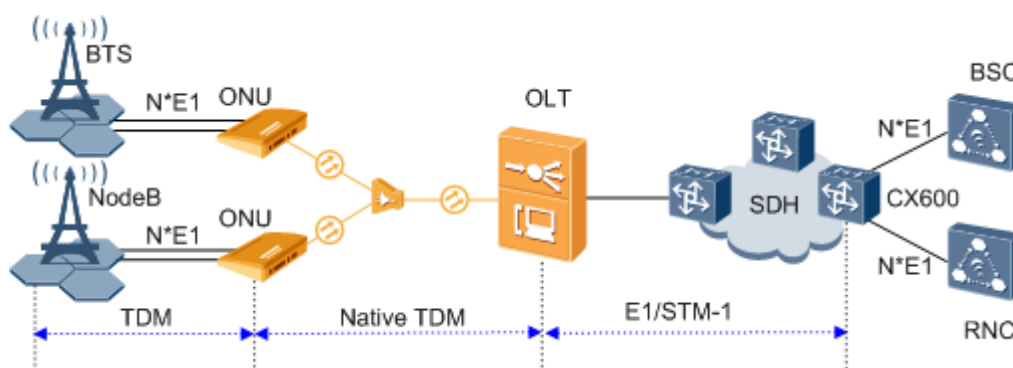
Service Requirements

- The E1 port is used for connecting to the 2G or 3G base station in a unified manner.
- GPON is adopted for bearing the mobile AN in a unified manner to meet mobile carriers' requirements for high bandwidth and high-density coverage of base stations.
- Make full use of existing SDH resources to transmit the TDM service with high quality.

Figure 4-8 shows an example network of the Native TDM base station access service.

The ONU is connected to the 2G or 3G base station through the E1 port to provide the TDM access, and then transmits the service data upstream to the GPON service board of 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) of the TOPA board. In this way, the 2G or 3G base station access service is implemented between the ONU and the OLT in the native TDM mode.

Figure 4-8 Native TDM base station access service



Data Plan

Table 4-4 provides the data plan for the OLT, and Table 4-5 provides the data plan for the ONU.

Table 4-4 Data plan for configuring the Native TDM base station access service-OLT side

Item	Data
VLAN	Inband management VLAN: smart VLAN 8 WARNING When the ONU is connected to the E1 service in native TDM mode, the system always uses VLANs 4000-4007. Hence, these VLANs should not be used in VLAN planning for the OLT or ONU. If these VLANs are used, ONU configuration fails. Consequently, services will be interrupted.
IP address	Inband management IP address: 192.168.50.1/24
GPON service board	Port: 0/3/1 ONU ID: 1 ONU authentication mode: SN ONU SN: 48575443E6D8B541
TOPA service board	Port: 0/5/0 Daughter board type: NH1A (providing E1 ports) or O2CE (providing STM-1 ports) VC12 ID: 2 (for only the STM-1 port)
DBA profile	Profile name: TDM Type: type1 Fixed bandwidth: 32 Mbit/s Dynamic bandwidth allocation mode of GPON ports: minimum bandwidth delay
ONU line profile	<ul style="list-style-type: none"> ● Profile ID: 11 ● GEM port ID: 1 ● T-CONT ID: 1 ● Bind T-CONT 1 to the DBA profile named TDM
ONU service profile	Profile ID: 11 Port type and quantity: 5 ETH ports, 8 E1 ports, and 8 POTS ports TDM port type: E1
ONU management mode	OMCI

Table 4-5 Data plan for configuring the Native TDM base station access service-ONU side

Item	Data
E1 port	Accessing base station signals on E1 port 1

Procedure

- **Configure the OLT.**

1. Configure GPON ONU profiles.

GPON ONU profiles include the DBA profile, line 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.
- 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 DBA profile name to TDM, type to type1, fixed bandwidth to 32 Mbit/s, and enable the bandwidth compensation. Configure the GPON dynamic bandwidth allocation mode of GPON port 0/3/1 to minimum bandwidth delay.

To configure the DBA profile of fixed bandwidth type to bear the TDM services, you must enable the bandwidth compensation function and configure the dynamic bandwidth allocation mode of the GPON port to minimum bandwidth delay.

```
huawei(config)#dba-profile add profile-name TDM type1 fix 32768
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
```

- b. Add an ONU line profile.

Add GPON ONU line profile 11, and bind T-CONT 1 to DBA profile named TDM.

```
huawei(config)#ont-lineprofile gpon profile-id 11
huawei(config-gpon-lineprofile-11)#tcont 1 dba-profile-name TDM
```

Add GEM port 1 for transmitting TDM traffic streams. Bind GEM port 1 to T-CONT 1. Configure the QoS mode to priority-queue (default) and the queue priority to 0 (highest priority).

```
huawei(config-gpon-lineprofile-11)#gem add 0 eth tcont 0 priority-
queue 0
huawei(config-gpon-lineprofile-11)#gem add 1 tdm tcont 1 priority-
queue 0
```

Configure the mapping mode from the GEM port to ONU-side service to VLAN (default), map the E1 port 1 of the ONU to GEM port 1.

```
huawei(config-gpon-lineprofile-11)#gem mapping 1 1 e1 1
```

After the configuration is complete, run the **commit** command to make the configured parameters take effect.

```
huawei (config-gpon-lineprofile-11) #commit
huawei (config-gpon-lineprofile-11) #quit
```

c. Add an ONU service profile.

Add GPON ONU service profile 11, configure 5 ETH ports, 8 E1 ports, and 8 POTS ports, and set the TDM port type to E1 and service type to Native TDM for the ONU.

```
huawei (config) #ont-srvprofile gpon profile-id 11
huawei (config-gpon-srvprofile-11) #ont-port eth 5 tdm 8 tdm-type e1
tdm-srvtype
tdmogem pots 8
huawei (config-gpon-srvprofile-11) #commit
huawei (config-gpon-srvprofile-11) #quit
```

d. (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 addgpon alarm-profile add** command to add an alarm profile, which is used for monitoring the performance of an activated ONU line.

2. 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.

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 485754434224C902 omci
ont-lineprofile-id
11 ont-srvprofile-id 11
```

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          :
2
```

```
F/S/P          :  
0/3/1  
Ont SN        :  
485754434224C902  
//The rest of the response information is omitted.
```

```
huawei(config-if-gpon-0/3)#ont confirm 1 ontid 1 sn-auth  
485754434224C902 omci ont-lineprofile-id  
11 ont-srvpofile-id 11
```

NOTE

If multiple ONUs of the same type are connected to a port and the same line profile or service profile (for an ONT) 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 ONU_0/3/1`.

- b. (Optional) Bind the alarm profile to the ONU.

The default profile (profile 1) is used.

```
huawei(config-if-gpon-0/3)#ont alarm-profile 1 1 profile-id 1
```

3. 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.
```

If the ONU state fails, the ONU fails to be in the up state, or the ONU does not match, refer to the following suggestions to rectify the fault.

- 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.

4. 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 192.168.50.1/24.

```
huawei (config-if-gpon-0/3) #quit
huawei (config) #vlan 8 smart
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.

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 static ip-address
192.168.50.2 mask 255.255.255.0 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-if-gpon-0/3) #quit
huawei (config) #service-port 0 vlan 8 gpon 0/3/1 ont 1 gempport 0 multi-
service
user-vlan 8 rx-cttr 6 tx-cttr 6
```

5. 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.
6. Configure the TDM connection.

Set up a native TDM connection between GEM port 1 and upstream port 0/5/0 of the TPOA board.

- In the case of the E1 upstream port, the configuration is as follows:

```
huawei (config) #tdm-connect connectid 1 tdm 0/5/0 gpon 0/3/1 ontid 1
gempportIndex 1
```

- In the case of the STM-1 upstream port, you must configure the VC12 parameter. VC12 is the virtual container that carries the E1 service. One STM-1 port contains 63 E1 ports. Accordingly, there are 63 VC12 virtual containers. The configuration is as follows:

```
huawei (config) #tdm-connect connectid 1 tdm 0/5/0 vc12 2 gpon 0/3/1
ontid 1 gempportIndex 1
```

7. Configure the system clock and time synchronization.

For details, see [4.1.3 Configuring E1/STM-1 Line Clock Synchronization](#).

8. Configure network protection.

For details, see [4.2 Configuring Base Station Access Network Protection](#).

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. The priority of the TDM emulation service is 6, adopting the PQ scheduling.

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
```

- **Configure the ONU.**

The ONU need not be configured. All the configurations are performed on the OLT and issued to the ONU through the OMCI protocol.

----End

Result

Mobile terminals (mobile phones) near the base station can obtain their network information normally and make calls and send messages to each other normally.

Configuration File

Configure the OLT.

```
vlan 8 smart  
interface vlanif 8  
ip address 192.168.50.1 24  
quit  
dba-profile add profile-name TDM type1 fix 32768 bandwidth_compensate yes  
interface gpon 0/3  
port dba bandwidth-assignment-mode 1 min-loop-delay  
quit  
ont-lineprofile gpon profile-id 11  
tcont 1 dba-profile-name TDM  
gem add 1 tdm tcont 1 priority-queue 0  
gem mapping 1 1 e1 1  
commit  
quit  
ont-srvprofile gpon profile-id 11  
ont-port eth 5 tdm 8 tdm-type e1 tdm-srvtype tdmogem pots 8  
commit  
quit  
interface gpon 0/3
```

```
port 1 ont-auto-find enable
ont confirm 1 ontid 1 sn-auth 485754434224C902 omci ont-lineprofile-id
  11 ont-srvpofile-id 11
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 gempport 0 multi-service
  user-vlan 8 rx-cttr 6 tx-cttr 6
tdm-connect connectid 1 tdm 0/5/0 gpon 0/3/1 ontid 1 gempportIndex 1 //E1 upstream
tdm-connect connectid 1 tdm 0/5/0 vc12 2 gpon 0/3/1 ontid 1 gempportIndex 1 //STM-1
upstream
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
```

4.5 Configuring the QinQ Private Line Base station access Service for the OLT

The ONU is connected to the IP-based station through the FE/GE port and the OLT transmits the QinQ private line service to the MAN device, implementing the base station access service. The ONUs support this service are MA5628.

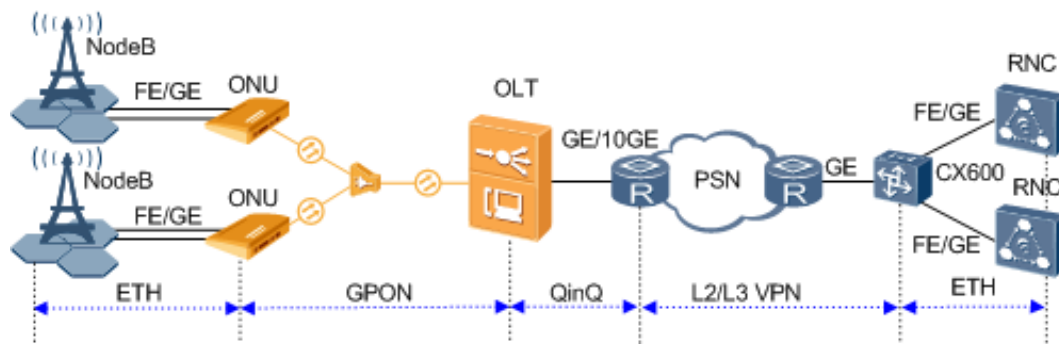
Service Requirements

- The ONU is connected to the 2G/3G base station and GPON is adopted for bearing the mobile access network in a unified manner, meeting mobile carriers' requirements for high bandwidth and high-density coverage of base stations.
- The service configuration adopts a simple and mature scheme, featuring a high transmission efficiency in addition to ensuring the QoS.

Figure 4-9 shows an example network of the QinQ private line base station access service on the OLT.

The ONU receives the ETH service data from the 3G base station through the FE/GE port, encapsulates the ETH packets into GEM frames, and then sends them to the OLT through the GPON upstream port. The OLT restores the ETH signals and configures the QinQ VLAN encapsulation mode so that the base station data can be transparently transmitted to the peer PTN through the public network. Finally, the PTN device restores the original ETH signals.

Figure 4-9 Example network of the QinQ private line base station access service



Data Plan

Table 4-6 provides the data plan for the OLT and **Table 4-7** provides the data plan for the ONU.

Table 4-6 Data plan for configuring the QinQ private line base station access service-OLT side

Item	Data
VLAN	Inband management VLAN: smart VLAN 8 SVLAN: smart VLAN 2000 with the attribute QinQ
IP address	Inband management IP address: 192.168.50.1/24
GPON service board	Port: 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 GEM Port ID: 0 and 1 T-CONT ID: 5 Bind T-CONT 5 to the DBA profile named PrivateLine
ONU management mode	SNMP

Table 4-7 Data plan for configuring the QinQ private line base station access service-ONU side

Item	Data
VLAN	Inband management VLAN: smart VLAN 8, adding GPON upstream port 0/0/0 to this VLAN SVLAN: smart VLAN 2000 with the attribute common, adding GPON upstream port 0/0/0 to the VLAN Tab of the ETH packets on the base station side: VLAN tag 20
ETH service port	0/4/0
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 VLAN 2000 and add upstream port 0/19/0 to it.


```
huawei(config)#vlan 2000 smart
huawei(config)#vlan attrib 2000 q-in-q
huawei(config)#port vlan 2000 0/19 0
```

2. Enable the transparent transmission of protocol packets for VLAN 2000.

- Enable the protocol packet forwarding switch.

By default, the protocol packet forwarding switch is enabled. Therefore, you need not configure this function.

```
huawei(config)#protocol permit-forwarding eapol enable
huawei(config)#protocol permit-forwarding efm enable
huawei(config)#protocol permit-forwarding lacp enable
huawei(config)#protocol permit-forwarding mstp enable
```

- 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.

```
huawei(config)#bpdu tunnel vlan 2000 enable
```

3. Configure the 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 DBA profile name to PrivateLine, profile type to type1, 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 MDU line profile 10, bind T-CONT 5 to DBA profile named PrivateLine. 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 PrivateLine
```

Add GEM port 0 for transmitting management traffic streams and GEM port 1 for transmitting ETH service 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.

 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
```

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, and map the service port of SVLAN 20 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 20
```

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-
lineprofile-id
10
```

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
//The rest of the response information is omitted.
huawei(config-if-gpon-0/3)#ont confirm 1 ontid 1 sn-auth 48575443E6D8B541
snmp ont-lineprofile-id
10
```

 **NOTE**

If multiple ONUs of the same type are connected to a port and the same line profile or service profile (for an ONT) 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: **ont confirm 1 all sn-auth snmp ont-lineprofile-id 10**.

- b. (Optional) Bind the alarm profile to the ONU.

The default profile (profile 1) is used.

```
huawei(config-if-gpon-0/3)#ont alarm-profile 1 1 profile-id 1
```

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.
```

If the ONU state fails, the ONU fails to be in the up state, or the ONU does not match, refer to the following suggestions to rectify the fault.

- 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 192.168.50.1/24.

```
huawei(config-if-gpon-0/3)#quit
huawei(config)#vlan 8 smart
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.

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 static ip-address
192.168.50.2 mask 255.255.255.0 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-if-gpon-0/3)#quit
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. Add the service port.

Configure the service port ID to 1, SVLAN ID to 2000, GEM port ID to 1, and CVLAN ID to 20. Rate limitation for upstream and downstream packets 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 2000 gpon 0/3/1 ont 1 gemport 1 multi-
service
user-vlan 20 tag-transform default 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. The priority of the TDM emulation service is 6, adopting the PQ scheduling.

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. Configure network protection.

For details, see [4.2 Configuring Base Station Access Network Protection](#).

11. 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. Create an SVLAN and add an upstream port to it.

The selection of SVLAN is flexible, which is mainly based on the VLAN switching policy of the ONU for base station packets.

- After VLAN switching, if the VLAN tag of the ONU upstream packet is the same as the VLAN tag of the base station, configure the SVLAN to be the same as the base station VLAN.
- After VLAN switching, if the VLAN tag of the ONU upstream packet is not the same as the VLAN tag of the base station, the SVLAN can be different from the base station VLAN.
- In both cases, the SVLAN of the ONU must be the same as the user-side VLAN on the OLT.

In this example, the ONU SVLAN is the same as the base station VLAN.

Configure the SVLAN ID to 20, type to smart, attribute to common, and upstream port to 0/0/0.

```
huawei(config)#vlan 20 smart  
huawei(config)#port vlan 20 0/0 0
```

2. Create 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 10, with the assured data rate 10240 kbit/s, priority 4, and priority strategy of scheduling by the priority in the packets.

```
huawei(config)#traffic table ip index 10 cir 10240 priority 4 priority-policy tag-In-Package
```

3. Create an ETH service port.

Create an ETH service port for VLAN 20. Perform VLAN switching (in this example, the VLAN tag remains the same after switched) on the base station packets from ETH port 0/4/0 and then transmit them to the OLT through an upstream port. In addition, use traffic profile 10.

```
huawei(config)#service-port vlan 20 eth 0/4/0 multi-service user-vlan 20
rx-cttr 10 tx-cttr 10
```

4. Save the data.

```
huawei(config)#save
```

---End

Result

Mobile terminals (mobile phones) near the base station can obtain their network information normally, make calls, and send messages to each other normally.

Configuration File

Configure the OLT.

```
vlan 2000 smart
vlan attrib 2000 q-in-q
port vlan 2000 0/19 0
protocol permit-forwarding eapol enable
protocol permit-forwarding efm enable
protocol permit-forwarding lacp enable
protocol permit-forwarding mstp enable
bpdu tunnel vlan 2000 enable
vlan 8 smart
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
mapping-mode vlan
gem mapping 0 0 vlan 8
gem mapping 1 1 vlan 20
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
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 gempport 0 multi-service
user-vlan 8 rx-cttr 6 tx-cttr 6
service-port 1 vlan 2000 gpon 0/3/1 ont 1 gempport 1 multi-service
user-vlan 20 tag-transform default 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 20 smart
port vlan 20 0/0 0
traffic table ip index 10 cir 10240 priority 4 priority-policy
tag-In-Package
```

```
service-port vlan 20 eth 0/4/0 multi-service user-vlan 20
  rx-cttr 10 tx-cttr 10
save
```

5 Configuring the FTTx Electric Power Applications

About This Chapter

This topic describes the configuration examples of transmitting video monitoring data, intelligently collecting power consumption information, and transmitting power distribution site information over the smart grid.

[5.1 Configuration Example of Transmitting Video Monitoring Data by Using the Ethernet Access](#)

The ONU can transmit video monitoring data through a gigabit Ethernet (GE)/fast Ethernet (FE) auto-adaptive electrical port.

[5.2 Configuration Example of Intelligently Collecting Power Consumption Information by Using the Ethernet Access](#)

The ONU can intelligently collect power consumption information in the electrical power system through a gigabit Ethernet (GE)/fast Ethernet (FE) auto-adaptive electrical port.

[5.3 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.

[5.4 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.

[5.5 Configuration Example of Automatically Transmitting Site Information over Ethernet \(Independent Upstream Transmission\)](#)

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 dual PON ports independent upstream transmission to ensure service reliability. GPON is the acronym for gigabit-capable passive optical network.

5.6 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.

5.1 Configuration Example of Transmitting Video Monitoring Data by Using the Ethernet Access

The ONU can transmit video monitoring data through a gigabit Ethernet (GE)/fast Ethernet (FE) auto-adaptive electrical port.

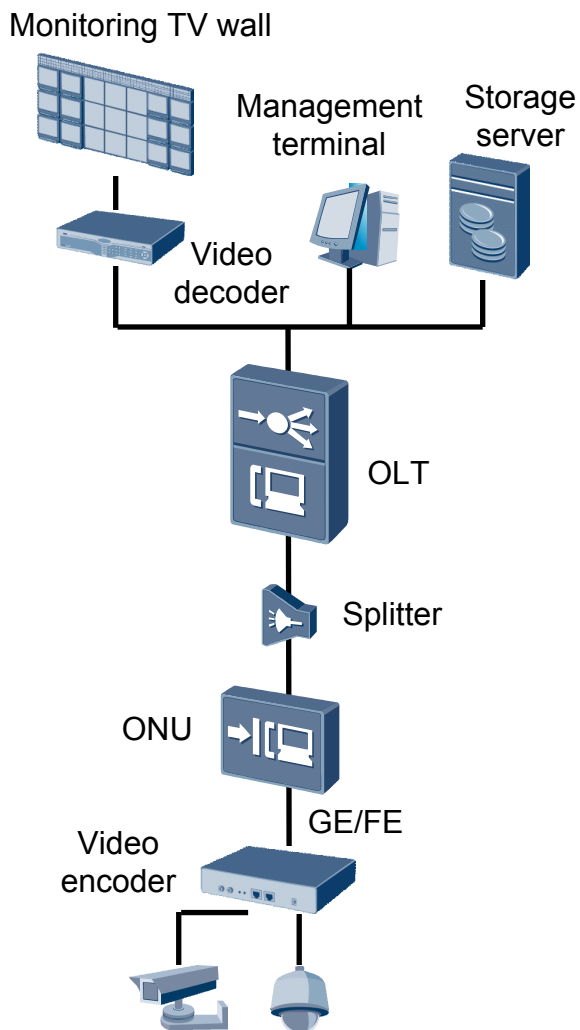
Service Requirements

- Located at a monitored point, the ONU is connected to video encoders through a GE/FE auto-adaptive electrical port. The ONU receives encoded video monitoring information and forwards the information upstream to an optical line terminal (OLT) at the monitoring center.
- The OLT forwards the information to other monitoring devices at the monitoring center.

Networking

Figure 5-1 shows the example network for configuring the video monitoring data transmission over Ethernet.

Figure 5-1 Example network for configuring the video monitoring data transmission over Ethernet



NOTE

This example uses MA5621 as the ONU.

Data Plan

Table 5-1 provides the data plan for the OLT, and **Table 5-2** provides the data plan for the ONU.

Table 5-1 Data plan for configuring the video monitoring data transmission over Ethernet-OLT side

Item	Data
VLAN	Inband management VLAN: smart VLAN 8 SVLAN: smart VLAN 100
IP address	Inband management IP address: 192.168.50.1/24

Item	Data
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 the DBA profile named VideoMonitoring GEM port IDs: 0, 1 T-CONT ID: 5
ONU management mode	SNMP

Table 5-2 Data plan for configuring the video monitoring data transmission over Ethernet-ONU side

Configuration Item	Data	Remarks
IP address	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 upstream port is used. In the case of multiple upstream ports, upstream link aggregation can be configured. For details, see *Configuring Upstream Link Aggregation*.

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 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 assured  
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.

 **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
```

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.

- 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 : V800R309C00
Ont EquipmentID  : SmartAX MA5621
Ont autofind time : 2011-03-10 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.
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.

- 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.
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 192.168.50.1/24.

```
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.

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 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:

```
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 192.168.50.1 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
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
```

5.2 Configuration Example of Intelligently Collecting Power Consumption Information by Using the Ethernet Access

The ONU can intelligently collect power consumption information in the electrical power system through a gigabit Ethernet (GE)/fast Ethernet (FE) auto-adaptive electrical port.

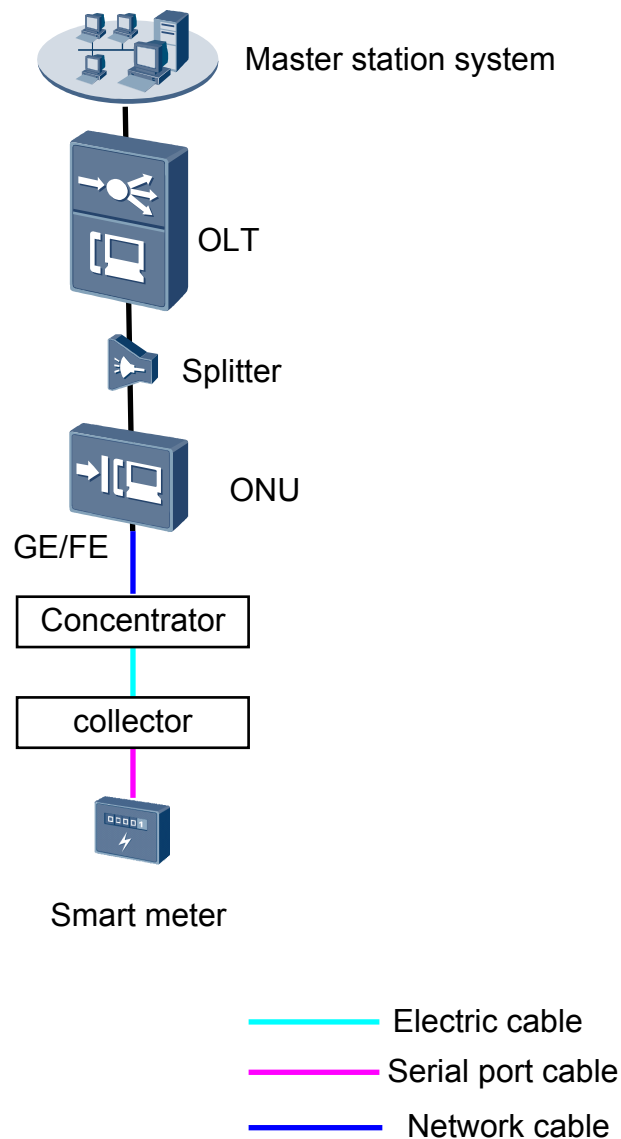
Service Requirements

- The ONU is connected to a concentrator through a GE/FE auto-adaptive 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 optical line terminal (OLT) and the OLT forwards the information to the upper-layer device. Then, the upper-layer device forwards the information to an automatic meter reading system (AMR) server.

Networking

Figure 5-2 shows the example network for configuring intelligent collection of power consumption information in the electrical power system over Ethernet.

Figure 5-2 Example network for configuring intelligent collection of power consumption information in the electrical power system over Ethernet



 **NOTE**

This example uses the MA5621 as the ONU.

Data Plan

Table 5-3 provides the data plan for the OLT, and **Table 5-4** provides the data plan for the ONU.

Table 5-3 Data plan for configuring intelligent collection of power consumption information in the electrical power system over Ethernet-OLT side

Item	Data
VLAN	Inband management VLAN: smart VLAN 8 SVLAN: smart VLAN 100
IP address	Inband management IP address: 192.168.50.1/24
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 the DBA profile named Data GEM port IDs: 0, 1 T-CONT ID: 5
ONU management mode	SNMP

Table 5-4 Data plan for configuring intelligent collection of power consumption information in the electrical power system over Ethernet-ONU side

Configuration Item	Data	Remarks
IP address	Inband management IP address: 192.168.50.2/24	
Traffic profile	Index 6 (default)	-
Service port	0/1/1	-
Uplink port	0/0/0	-

Configuration Item	Data	Remarks
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 upstream port is used. In the case of multiple upstream ports, upstream link aggregation can be configured. For details, see [Configuring Upstream Link Aggregation](#).

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
```

- 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.

 **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
```

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-
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 : V800R309C00
Ont EquipmentID : SmartAX MA5621
Ont autofind time : 2011-03-10 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.

- 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 192.168.50.1/24.

```
huawei(config)#vlan 8 smart
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.

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 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 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 gempport 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:  
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 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 5
tx-cttr 5
```

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
interface vlanif 8
ip address 192.168.50.1 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 0/1/1 multi-service user-vlan untagged rx-cttr 6 tx-
cttr 6
save
```

5.3 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.

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 *Feature Description*.

Service Requirements

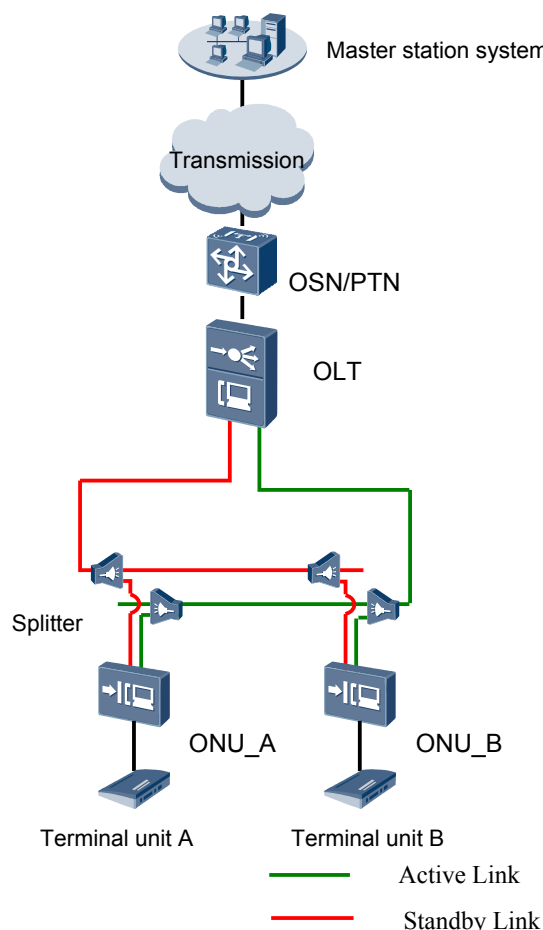
- In a smart grid, terminal units collect the running status information, as well as monitoring and control information about the power distribution system and send the information to the master station system.
- The information collected by terminal units is transparently transmitted to the master station 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 5-3 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.
- 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 5-3 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 5-5 provides the OLT data plan, and **Table 5-6** provides the ONU data plan.

Table 5-5 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	<ul style="list-style-type: none"> ● 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.	<ul style="list-style-type: none"> ● Port: <ul style="list-style-type: none"> - 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	<ul style="list-style-type: none"> ● Profile name: Data ● Type: type3 ● Assured bandwidth: 20 Mbit/s ● Maximum bandwidth: 50 Mbit/s
	ONU line profile	<ul style="list-style-type: none"> ● 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

Device	Item	Data
	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 5.

Table 5-6 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	<ul style="list-style-type: none"> ● 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 <ul style="list-style-type: none"> ● 0/0/0: active uplink port ● 0/0/1: standby uplink port 	-
	Uplink VLAN	<ul style="list-style-type: none"> ● 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.	-

Device	Configuration Item	Data	Remarks
	User-side VLAN	<ul style="list-style-type: none"> ● 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.
- 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
```

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.

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 : 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.
-----
```

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) #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.

```
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
  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

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	-
- 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
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     :
-
  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.

```
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.

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
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 gempport 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 gempport 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 gempport 2 multi-service
user-vlan 100 gempport 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
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
```

5.4 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.

Background Information

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. For details about the GPON type C protection mechanism, see *Feature Description*.

Service Requirements

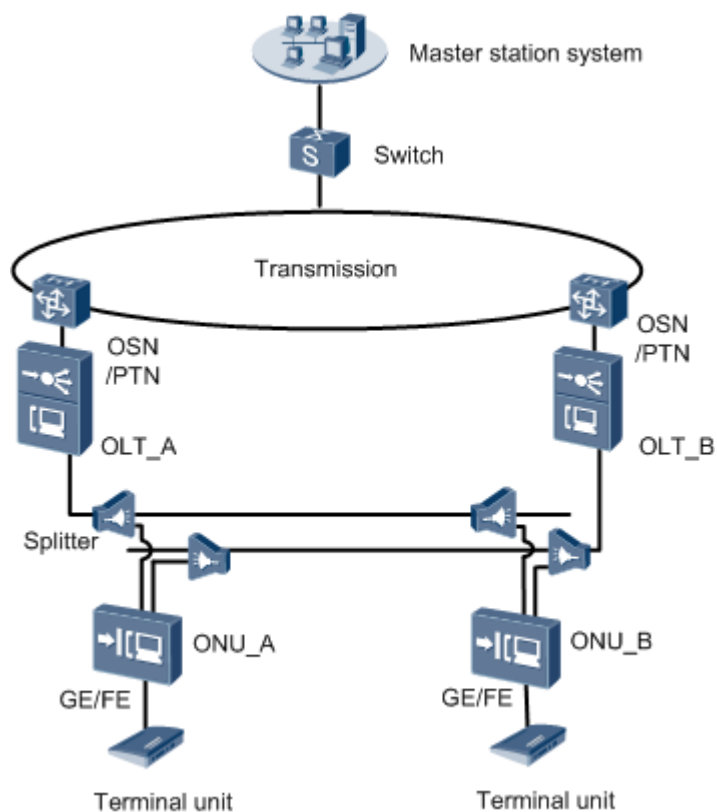
- In a smart grid, terminal units collect the running status information, as well as monitoring and control information about the power distribution system and send the information to the master station system.
- The information collected by terminal units is transparently transmitted to the master station 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 5-4 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 5-4 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.

Data Plan

Table 5-7 provides the OLT data plan, and **Table 5-8** provides the ONU data plan.

Table 5-7 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

Device	Item	Data
	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	<ul style="list-style-type: none"> ● 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.
OLT_B	The data plan is the same as that of OLT_A.	

Table 5-8 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	<ul style="list-style-type: none"> ● Index 10 (used for transmitting the power distribution site information) ● Index 11 (used for transmitting GOOSE packets) 	-
	Service port	Eth port: 0/1/1	-

Device	Configuration Item	Data	Remarks
	Uplink port	GPON port: 0/0/0, 0/0/1	-
	Uplink VLAN	<ul style="list-style-type: none"> 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.	-
	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.
- 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
```

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.

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 : 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.
```

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)#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.

```
huawei(config)#service-port 0 vlan 8 gpon 0/3/1 ont 1 gempport 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**

Run the **protect-group member port 0/3/1 ont 1 role protect** command on OLT_B to set the group member status to protect. Other configurations on OLT_B are the same as these 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
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.Ip 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   :
-
  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 gempport 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 gempport 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.

```
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
-
  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. 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
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 dual-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 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              :
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.

```
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
```

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
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
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
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
```

5.5 Configuration Example of Automatically Transmitting Site Information over Ethernet (Independent Upstream Transmission)

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 dual PON ports independent upstream transmission to ensure 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.

In the GPON line independent upstream transmission mechanism, the two PON lines between an ONU and an OLT are in the working state and can forward packets at the same time. The two lines transmit and receive packets between the terminal unit and the electrical power system independently. No switching occurs and no protection group is required on the OLT. For details about the independent upstream transmission mechanism, see *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.

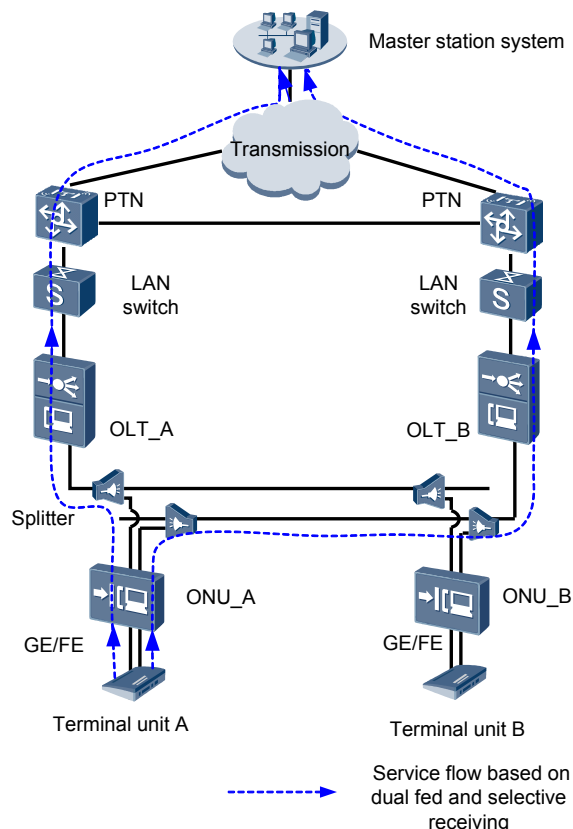
- The information is transmitted over a GPON network.

Networking

Figure 5-5 shows an example network for configuring the automatic transmission of power distribution site information in the electrical power system over Ethernet. In the figure, the blue dashed line represents service flow based on the dual fed and selective receiving function between terminal unit A 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.
- 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.
- The site information and GOOSE services must be configured on ONU_A and ONU_B so that they can be transmitted to OLT_A and OLT_B at the same time.

Figure 5-5 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 5-9 provides the OLT data plan, and **Table 5-10** provides the ONU data plan.

Table 5-9 Data plan for configuring automatic transmission of 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 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 300 (used for transmitting GOOSE packets)
	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: Data Type: type3 Assured bandwidth: 20 Mbit/s Maximum bandwidth: 50 Mbit/s
	ONU line profile	<ul style="list-style-type: none"> ● 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 the information about the electrical power system) ● GEM port ID: 2 (used for transparently transmitting GOOSE packets) ● T-CONT ID: 5 <p>NOTE In GPON independent upstream transmission scenarios, an OLT supports a maximum of eight T-CONTs.</p>
	ONU management mode	SNMP

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 6.
OLT_B	The data plans for OLT_A and OLT_B are the same except for the SVLAN ID and IP address. NOTE The two OLTs require the same hardware and software versions, including the versions of GPON service boards. The control board of the OLTs must be SCUN and the GPON service board can be an H801GPBC, H802GPBD, or H805GPBD board.	
	VLAN	Inband management VLAN: smart VLAN 8 CVLAN: smart VLAN 201; SVLAN: smart VLAN 201 (used for transmitting the site information about the electrical power system) CVLAN: smart VLAN 101; SVLAN: smart VLAN 301 (used for transmitting GOOSE packets)
	Inband management IP address	192.168.50.10/24

Table 5-10 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	<ul style="list-style-type: none"> ● Index 10 (used for transmitting the power distribution site information) ● Index 11 (used for transmitting GOOSE packets) 	-
	Service port	Ethernet port: 0/1/1, 0/1/2	Ports 0/1/1 and 0/1/2 are used for two services on terminal unit A.

Device	Configuration Item	Data	Remarks
	Uplink port	GPON port: 0/0/0, 0/0/1	Port 0/0/0 connects to the service port on OLT_A and port 0/0/1 connects to the service port on OLT_B.
	Uplink VLAN	<ul style="list-style-type: none"> ● Smart VLAN 8 (used for transmitting inband management service stream) ● ONU_A to OLT_A: <ul style="list-style-type: none"> - Smart VLAN 200 (used for transmitting power distribution site information) - Smart VLAN 100 (used for transmitting GOOSE packets) ● ONU_A to OLT_B: <ul style="list-style-type: none"> - Smart VLAN 201 (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.	-
	User 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 ID of the uplink VLAN used for transmitting power distribution site information and IP address.		

Procedure

Step 1 Configure OLT_A.

1. Create an SVLAN and add an uplink port to it.

Create smart VLANs 200 300, and add uplink port 0/19/0 to VLAN 200.

```
huawei(config)#vlan 200 smart
huawei(config)#port vlan 200,300 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
```

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.

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              :
VendorID              : 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.
```

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)#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.

```
huawei(config)#service-port 0 vlan 8 gpon 0/3/1 ont 1 gempport 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 site information service port ID to 1, SVLAN ID to 200, GEM port ID to 1, CVLAN ID to 200 and configure the GOOSE packets service port ID to 2, SVLAN ID to 300, GEM port ID to 2, CVLAN ID to 100. 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 uplink VLAN on 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                 :
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 gempport 1 multi-
service
user-vlan 200 inbound traffic-table index 20 outbound traffic-table index 20
huawei(config)#service-port 2 vlan 300 gpon 0/3/1 ont 1 gempport 2 multi-
service
user-vlan 100 inbound traffic-table index 21 outbound traffic-table index 21

```

9. 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

```

```
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	-
- 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 300 profile-id 20
```

10. 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
```

11. Save the data.

```
huawei(config)#save
```

Step 2 Configure OLT_B.

1. Create an SVLAN and add an uplink port to it.

Create smart VLANs 201 301, and then add uplink port 0/19/0 to VLAN 201.

```
huawei(config)#vlan 201,301 smart
huawei(config)#port vlan 201 0/19 0
```

2. Add an ONU on the OLT by referring to [Step 1.3](#) through [Step 1.5](#).

3. Configure the management channel from the OLT to the ONU.

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 192.168.50.10/24.

```
huawei(config-if-epon-0/3)#quit
huawei(config)#vlan 8 smart
```

```
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 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
huawei(config-if-gpon-0/3)#quit
```

- 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
```

4. Create a service port.

Configure the site information service port ID to 1, SVLAN ID to 201, GEM port ID to 1, CVLAN ID to 201 and configure the GOOSE packets service port ID to 2, SVLAN ID to 301, GEM port ID to 2, 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 5.

The CVLAN must be the same as the uplink VLAN on 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              :
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 201 gpon 0/3/1 ont 1 gempport 1 multi-
service
user-vlan 201 rx-cttr 20 tx-cttr 20
huawei(config)#service-port 2 vlan 301 gpon 0/3/1 ont 1 gempport 2 multi-
service
user-vlan 101 rx-cttr 21 tx-cttr 21
```

5. 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
```

```
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      -
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 301 profile-id 20
```

6. 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
```

Step 3 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
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 independent upstream transmission.

Set the dual PON ports independent upstream transmission mode to **Independent uplink mode**.

```
huawei(config)#pon uplink-mode independent
```

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      :
    -
    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 OLT_A.
huawei(config)#vlan 101,201 smart ///Create SVLANs for service
transmission from ONU_A to OLT_B.
```

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
huawei(config)#port vlan 101,201 0/0 1
```

6. Create service ports.

- Create a service port for the transmission from ONU_A to OLT_A.

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
```

- Create a service port for the transmission from ONU_A to OLT_B.

For power distribution site information, create service port 4 with SVLAN 201 and traffic profile 10.

```
huawei(config)#service-port 4 vlan 201 eth 0/1/2 multi-service user-vlan
untagged
rx-cttr 10 tx-cttr 10
```

For GOOSE packets, create service port 5 with SVLAN 101, CVLAN 2, and traffic profile 11.

```
huawei(config)#service-port 5 vlan 101 eth 0/1/2 multi-service user-vlan 2
rx-cttr 11 tx-cttr 11
```

7. Disable the unknown multicast suppression function.

Goose packets are unknown multicast packets. Disable the unknown multicast suppression function on the ONU 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
```

8. 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
```

9. 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 100,101 profile-id 10
```

10. 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)#undo traffic-suppress 2 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
```

11. 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
```

12. 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.

Configuration File

Configure OLT_A.

```
vlan 200,300 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 300
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
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
quit
service-port 0 vlan 8 gpon 0/3/1 ont 1 gempport 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
traffic table ip index 21 cir off priority 5 priority-policy local-Setting
service-port 1 vlan 200 gpon 0/3/1 ont 1 gempport 1 multi-service
user-vlan 200 inbound traffic-table index 20 outbound traffic-table index 20
service-port 2 vlan 300 gpon 0/3/1 ont 1 gempport 2 multi-service
user-vlan 100 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 300 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 OLT_B.

```
vlan 201,301 smart
port vlan 201 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 201
gem mapping 2 2 vlan 301
commit
quit
interface gpon 0/3
port 1 ont-auto-find enable
ont add 1 1 sn-auth 48575443E6D8B541 snmp ont-lineprofile-id
  10 desc MA5621_0/3/1/1_lineprofile10
quit
vlan 8 smart
interface vlanif 8
ip address 192.168.50.10 24
quit
interface gpon 0/3
ont ipconfig 1 1 ip-address 192.168.50.2 mask 255.255.255.0 manage-vlan 8
```

```
quit
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
traffic table ip index 21 cir off priority 5 priority-policy local-Setting
service-port 1 vlan 201 gpon 0/3/1 ont 1 gemport 1 multi-service
user-vlan 201 rx-cttr 20 tx-cttr 20
service-port 2 vlan 301 gpon 0/3/1 ont 1 gemport 2 multi-service
user-vlan 101 rx-cttr 21 tx-cttr 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 301 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 independent
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
vlan 101,201 smart
port vlan 100,200 0/0 0
port vlan 101,201 0/0 1
service-port 2 vlan 200 eth 0/1/1 multi-service user-vlan untagged
  rx-cttr 10 tx-cttr 10
service-port 3 vlan 100 eth 0/1/1 multi-service user-vlan 2 rx-cttr 11 tx-cttr 11
service-port 4 vlan 201 eth 0/1/2 multi-service user-vlan untagged
  rx-cttr 10 tx-cttr 10
service-port 5 vlan 101 eth 0/1/2 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 100,101 profile-id 10
interface eth 0/1
undo traffic-suppress 1 multicast
undo traffic-suppress 2 multicast
quit
interface eth 0/0
undo traffic-suppress all multicast
quit
queue-scheduler strict-priority
save
```

5.6 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

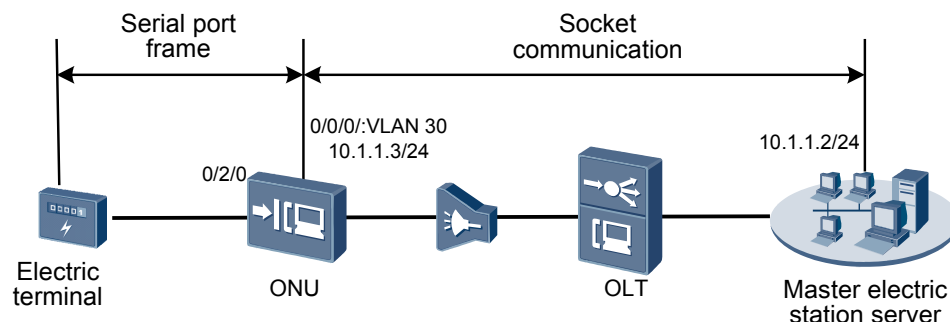
- In an electrical power system, a large amount of meter data needs to be collected in centralized mode in real time and sent to an automatic meter reading system (AMR) server for monitoring and processing.
- A user-side smart meter has a serial port, through which the ONU connects to the smart meter.
- Data is transmitted over a GPON network.

Networking

Figure 5-6 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 5-6 Network diagram for transmitting information collected in centralized mode in the smart grid over a serial port



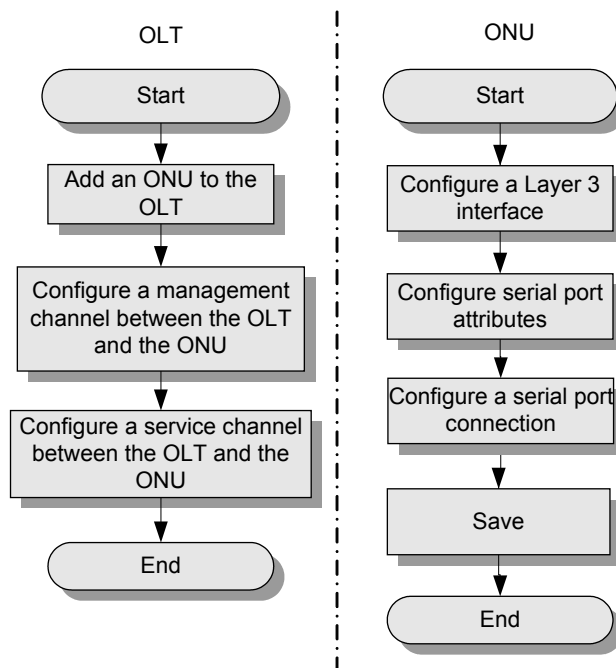
NOTE

This example uses an MA5621 as an ONU.

Configuration Flowchart

Figure 5-7 shows the flowchart for transmitting information collected in centralized mode in the smart grid over a serial port.

Figure 5-7 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.

Data Plan

Table 5-11 provides the data plan for the optical line terminal (OLT) and **Table 5-12** provides the data plan for the ONU.

Table 5-11 Data plan for the OLT

Configuration Item	Data
Virtual local area network (VLAN)	<ul style="list-style-type: none"> ● 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	<ul style="list-style-type: none"> ● Port ID: 0/3/1 ● ONT ID: 1 ● ONU authentication mode: SN ● ONU serial number (SN): 48575443E6D8B541
Dynamic bandwidth allocation (DBA) profile	<ul style="list-style-type: none"> ● Profile name: SerialAccess ● Type: type3 ● Assured bandwidth: 20 Mbit/s ● Maximum bandwidth: 50 Mbit/s
ONU line profile	<ul style="list-style-type: none"> ● 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 5-12 Data plan for the ONU

Configuration Item	Data	Remarks
Attributes of the inband management interface	<ul style="list-style-type: none"> ● 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) 	-

Configuration Item	Data	Remarks
Attributes of the VLAN Layer 3 interface	<ul style="list-style-type: none"> ● 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	<ul style="list-style-type: none"> ● Serial port ID: 0/2/0 ● Working mode: rs232 ● Baud rate: 9600 bit/s 	<p>The default value of the baud rate is 9600 bit/s.</p> <p>Ensure that the serial port attributes are the same as those on the interconnected terminal unit.</p>
Connections of the serial port	<ul style="list-style-type: none"> ● Connection ID: 1 ● Transmission mode: tcp-server ● Local port ID: 3000 ● Serial port frame type: ft1.2 	<p>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.</p> <p>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.</p>

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.

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 assured
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.

- 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         :
VendorID         : 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 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
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 gempport 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              :  
off  
CBS              :  
off  
PIR              :  
off  
PBS              :  
off  
Referenced Status : not  
used  
-----
```

```
huawei(config)#service-port 1 vlan 30 gpon 0/3/1 ont 1 gempport 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.

```
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 RS232, 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 rs232
```

4. (Optional) Configure serial port attributes.

The default value of the serial port baud rate is 9600 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 9600
```

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 10.10.1.3, and serial port frame type to ft1.2.

```
huawei(config)#serialop-connection 1 port 0/2/0 working-mode tcp-server local-address
10.1.1.3 local-port 3000 peer-address 10.10.1.3 frame-type ft1.2
```

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
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 rs232
interface serial 0/2
port config 0 baudrate 9600
serialop-connection 1 port 0/2/0 working-mode tcp-server local-address
 10.1.1.3 local-port 3000 peer-address 10.10.1.3 frame-type ft1.2
save
```

6 Configuring Example of EoC Broadband Services

This topic describe how to configure Ethernet over coaxial cable (EoC) broadband services. The ONUs used in this application scenario include MA5631, MA5632. Here, the MA5631 is used as an example.

Prerequisites

Before configuring broadband services, ensure that the coaxial network unit (CNU) and the EoC head end module are connected properly. For details about the configuration of the CNU.

Service Requirements

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.

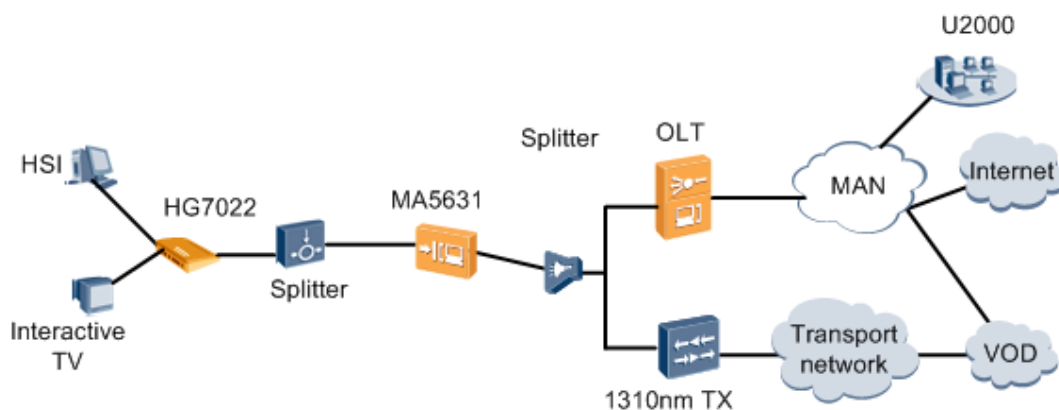
 **NOTE**

In Dynamic Host Configuration Protocol (DHCP) dialup mode, you can configure anti-theft and roaming for user accounts. For details.

Networking

Figure 6-1 shows a network diagram of the EoC broadband service.

Figure 6-1 Network diagram of the EoC broadband service



Data Plan

Table 6-1 provides the data plan for the OLT, and **Table 6-2** provides the data plan for the ONU.

Table 6-1 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 6-2 Data plan for configuring the EoC broadband service-ONU side

Item	Data
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
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.

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.

```
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.
- 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_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.
```

If the ONU configuration fails or the ONU fails to be up, check the ONU state by referring to the above-mentioned descriptions.

- 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 log in to the ONU using the Telnet 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-if-gpon-0/3) #quit
huawei (config) #vlan 8 smart
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.
- 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 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 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.

NOTE

Because the management VLAN and the management IP address have been configured, 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 using 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. The user name is **root** (default) and the password is **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. 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
```

3. 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

4. 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
```

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
```

5. 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
```

6. 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
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
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.

```
vlan 100-101 smart
vlan attrib 100 stacking
vlan attrib 101 common
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 100 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
stacking label service-port 100 2
```

```
service-port 101 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
```